Driving innovation together

DPIA Adobe Creative Cloud & Document Cloud

SURF

Author(s): Sanne Ouburg, Mike Noordermeer, Jacob Gursky, Winfried Tilanus, Floor Terra
Version: 1.01
Date: 12 February 2026

Version history

Version	Date	Summary of changes
0.1	20 November 2024	Internal partial draft part A.
0.2	7 February 2025	First draft part A.
0.25	19 February 2025	Second draft part A – incorporated feedback SURF and input Adobe on all questions asked.
0.3	9 May 2025	Draft part A and B.
0.4	14 May 2025	Full draft (excluding conclusion).
0.5	28 November 2025	Processed feedback by Adobe. Several risks removed or reclassified. Post-mitigation risk ratings and further context added.
0.9	13 January 2026	Processed feedback by Adobe. Several risks removed or reclassified. Summary and Conclusion added.
1.0	28 January 2026	Processed feedback by Adobe. Amended Summary and Conclusion.
1.01	12 February 2026	Amended Summary and Conclusion after Adobe feedback. Adjusted document formatting and spelling.

Glossary of key terms

Admin: *"an administrator who manages the Services and Software for Business Users within your Business"*. [1]

Admin Console: *"the program administration user interface that allows Admins to manage their Business's Services and Software"*.[2]

Adobe ID: Identity type on Adobe Admin Console. *"Created, owned, and managed by the end user. Adobe performs the authentication, and the end user manages the identity. Depending upon the storage model, users or businesses retain control over files and data. Adobe ID accounts are created on unverified, public, or trusted domains"*.[3]

Adobe Identity Data: *"This is operational data about Adobe account activity, such as logins, changes made to user account information, when an account is added to an organization, and when an organization makes changes to its users' accounts"*.[4]

Child: a natural person below the age of eighteen years (Article 1 of the United Nations Convention on the Rights of the Child).

Children's consent: consent given by a person under the age of 18 who has reached the age of digital consent pursuant to Article 8 GDPR. This age may vary between Member States: from 13 to 16 years. In the Netherlands, until children are 16, their parents/legal guardians must provide consent where required.

Consent: 'consent' of the data subject means 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 (Article 4 (11) GDPR).

Consent mechanism: a method of obtaining consent of the data subject, for example through pop-ups and banners.

Consortium: SurfMarket B.V. who has entered into a sales order with Adobe for the purchase of Products and Services and is authorized to make the Products and Services identified in the sales order available to Consortium Member.

---

[1] Article 1.1, Business Product Specific Terms, Published October 7, 2024 URL:
https://wwwimages2.adobe.com/content/dam/cc/en/legal/servicetou/Business-Product-Specific-Terms-en-US-20241007.pdf.

[2] Article 1.2, Business Product Specific Terms, Published October 7, 2024 URL:
https://wwwimages2.adobe.com/content/dam/cc/en/legal/servicetou/Business-Product-Specific-Terms-en-US-20241007.pdf.

[3] https://helpx.adobe.com/enterprise/using/identity.html#using-personal-adobe-id, last viewed 11 November 2024.

[4] Adobe DSAR Response of 30 October 2024, p. 7.

Consortium Member: that educational institution that meets the education eligibility criteria for Adobe's education programs[5] and those entities that meet the Adobe not for profit[6] and are either listed under Exhibit B of the Sales Order or added at the agreed Entry Points.

Content: "any text, information, communication, or material, such as audio files, video files, electronic documents, or images, that you upload, import into, embed for use by, or create using the Services and Software".[7]

(Data) controller: 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 4 (7) GDPR).

(Data) processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4 (8) GDPR).

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 (Article 4 (1) GDPR).

Enterprise ID: Created, owned, and managed by the organization. *"The organization retains exclusive rights to create user accounts on verified domains"*. [8]

ETLA: Enterprise Term License Agreement.

Federated ID: Identity type on Adobe Admin Console*. "Created, owned, and managed by the organization. The organization manages user-credentials and uses Single Sign-On (SSO) via a SAML2 identity provider (IdP)"*.[9]

Fonts Data: *"This contains information about your use of Adobe fonts, capturing certain types of activity (e.g., font used)"*.[10]

Information society service: any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (Article 4 (25) GDPR and point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council).

---

[5] Described at Adobe, Primary and Secondary Institution Eligibility Guidelines, Last updated 16 December 2024, URL: https://www.adobe.com/fragments/textandimage/education/edu-ste-eligibility-institutions.html.

[6] Criteria available at https://helpx.adobe.com/ie/enterprise/using/non-profit.html.

[7] Article 4.1, Adobe General Terms of Use, Effective as of June 18, 2024, URL: https://www.adobe.com/legal/terms.html#content.

[8] https://helpx.adobe.com/enterprise/using/identity.html#using-personal-adobe-id, last viewed 11 November 2024.

[9] https://helpx.adobe.com/enterprise/using/identity.html#using-personal-adobe-id, last viewed 11 November 2024.

[10] Adobe DSAR Response of 30 October 2024, p. 6.

Integrity Data: *"Integrity data comes from a service incorporated into the code of Adobe desktop applications that serves to capture certain information about the software license and the device on which it is installed in order to help prevent the pirating of genuine Adobe software"*.[11]

K-12: refers to primary and secondary education (from kindergarten to 12th grade).

Managed Services: "the technology services hosted by or on behalf of Adobe and provided to Customer as a dedicated instance, as set out in the Sales Order."[12]

National Center for Missing and Exploited Children (NCMEC): The National Center for Missing & Exploited Children (NCMEC) is a private, nonprofit organization, acts as an information clearinghouse and resource for parents, children, law enforcement agencies, schools, and communities to assist in locating missing children and to raise public awareness about ways to prevent child abduction, and child sexual abuse.[13]

On-demand Services: "the technology services hosted by or on behalf of Adobe and provided to Customer as a shared instance, as set out in the Sales Order." [14]

On-premise Software: "the Adobe software that is deployed by or on behalf of Customer on hardware designated by Customer, as set out in the Sales Order." [15]

Parental consent: consent given or authorized by the parent or legal guardian of a child pursuant to Article 8 GDPR.

Participation Agreement: the form attached to SURF's Adobe Sales Order as Exhibit A which all eligible Consortium Members must execute prior to participation in the ETLA.[16]

Personal data: 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 (Article 4 (1) GDPR).

Portfolio Data: *"this contains data related to the Adobe Portfolio products assigned to your Adobe ID that users can have access to (e.g., Portfolio, Behance, Lightroom)"*.[17]

Processing: 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,

[11] Adobe DSAR Response of 30 October 2024, p. 7.

[12] Article 1.22, GENERAL TERMS (2024v1), URL: https://www.adobe.com/content/dam/cc/uk/legal/terms/enterprise/pdfs/GeneralTerms-UK-2024v1.pdf.

[13] https://www.missingkids.org/ourwork/impact.

[14] Article 1.23, GENERAL TERMS (2024v1), URL: https://www.adobe.com/content/dam/cc/uk/legal/terms/enterprise/pdfs/GeneralTerms-UK-2024v1.pdf.

[15] Article 1.24, GENERAL TERMS (2024v1), URL: https://www.adobe.com/content/dam/cc/uk/legal/terms/enterprise/pdfs/GeneralTerms-UK-2024v1.pdf.

[16] Article 4, Sales Order Terms, Adobe Contract Number 00818261.

[17] Adobe DSAR Response of 30 October 2024, p. 6.

structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4 (2) GDPR).

Product and Services Data: *"This is operational, cloud and user behavioral data for Adobe's Creative Cloud and Document Cloud, web, mobile and desktop apps and services. It is best understood as product usage data, showing how a particular user navigates and deploys Adobe products (e.g., individual Generative AI prompts)"*.[18]

Product Specific Licensing Terms (PSLT): means the Product Specific Licensing Terms document(s) that describe(s) the additional licensing terms for specific Products and Services. [19]

Profile data: *"This sets the basic information for your user profile (name, type of account, email)"*.[20]

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4 (4) GDPR).

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Article 4 (5) GDPR).

Reportable content: content that is Child Sexual Abuse Material matching the definition of "child pornography" under 18 USC § 2256(8).[21]

Sign Data: *"this contains data associated with Adobe Sign and your user Profile. It includes security verification data, dates of modification, some limited account activity and settings that are in place"*. [22]

[18] Adobe DSAR Response of 30 October 2024, p. 7.

[19] Article 1.27, Adobe General Terms (2024v1), (2024v1), Effective Date: 8 March 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf.

[20] Adobe DSAR Response of 30 October 2024, p. 6.

[21] Email Adobe to SURF of 11 February 2026.

[22] Adobe DSAR Response of 30 October 2024, p. 6.

Table of contents

Summary

This report is a data protection impact assessment (hereinafter: DPIA) on the use of Adobe's Creative Cloud and Document Cloud for Education by educational institutions (hereinafter: institutions). This DPIA is a central DPIA, carried out by Privacy Company on behalf of SURF, the ICT cooperative of Dutch education and research institutions, which provides institutions with a general framework for assessing data protection risks within Adobe Creative Cloud and Document Cloud for Education

Scope
This DPIA focuses on Adobe Creative Coud and Document Cloud for Education. Adobe's Creative Cloud for Education is a version tailored to the education sector and focused on adapting its safeguards to the needs and requirements of educational institutions. For example, Adobe has implemented privacy protections for educational users, including preventing these users from opting into personalized advertising cookies, which limits invasive data processing. Additionally, Adobe's system automatically identifies K-12 student email addresses and opts them out of marketing communications, ensuring these students receive only essential operational messages.

The DPIA assessed the contractual framework and the contractual provisions that were agreed upon during negotiations between SURF and Adobe in 2022, with certain terms reflecting SURF's preferences at that time. It is important to emphasize that risks relating to the contractual framework do not necessarily reflect a broader issue affecting Adobe in general. SURF and Adobe will address the flagged risks as part as the ongoing contract renewal negotiations that are taking place at this moment.

Methodology
Privacy Company combined a legal fact-finding strategy with a technical examination of the data processed through the use of the products. Privacy Company conducted its assessment using public information, the documentation about the system (as provided by Adobe) and by carrying out use-case scenarios within the products. Privacy Company subsequently submitted a data subject access request to Adobe in order to obtain insight into which personal data processing operations, including logging and telemetry, took place while these scenarios were executed. A technical analysis was also conducted to assess whether the observed data processing operations corresponded with the available documentation. Throughout 2025, several rounds of questions and feedback were undertaken on the report, including clarification of issues and working towards solutions. Adobe, SURF and Privacy Company also had a meeting to discuss Adobe's Trust and Safety measures, including its CSAM scanning methods and techniques. On the basis of all available information, this DPIA documents an assessment of whether the data processing operations result in risks to the rights and freedoms of data subjects.

Outcome and conclusion: 9 high risks, 8 low risks

This DPIA has identified 9 high risks and 8 low risks in the use of Adobe's Creative Cloud and Document Cloud. The main causes of these risks are:

- SURF's current contractual framework
- Product features that restrict data subjects from deleting or unsharing documents
- Limitations for administrators of institutions in being able to honour the rights of data subjects
- Disproportionate processing of Adobe's content credentials.

Throughout the DPIA process, Adobe demonstrated a highly constructive and collaborative approach, working closely with SURF to address all identified issues. Adobe assessed the feasibility of the requested technical mitigations and identified which measures it will implement, along with expected timelines. The completed measures have been incorporated into Part A of the DPIA and the corresponding risks from Part C and D have been removed. The planned or ongoing measures are included as scheduled mitigations in Part C and D. As a general clarification, Adobe noted that Adobe's commitments should not be interpreted as an acknowledgement of any legal obligation or agreement with the assigned risk levels, and that the improvements *"should instead be viewed in the spirit of making improvements requested by a specific customer with unique requirements due to the context of how they use Adobe services"*.[23] While not agreeing with all risk assessments or classifications, Adobe has expressed willingness to discuss specific contractual language on several points as part of the ongoing contract renewal negotiations.

Part D of this DPIA outlines technical and organisational measures that can be adopted by the educational institutions, Adobe, or both to mitigate all identified high risks. These measures are expected to reduce risks to a low residual level. In that case, no prior consultation with the Data Protection Authority is required. Although reducing low risks is not strictly necessary, it is recommended because the measures are easy to implement and help better protect the rights and freedoms of data subjects.

As a final note, Adobe Creative Cloud is used in schools to help students create digital art, design, video, and multimedia projects. In art schools or art courses where students explore experimental or provocative themes, educators should be aware that content involving non-reportable child sexualization and extreme sexual content (when reported) may conflict with Adobe's content policies, potentially resulting in account restrictions. Schools should therefore be familiar with these policies when using Adobe's products and services.

The table below provides an overview of the risks identified in this DPIA, the suggested measures for educational institutions, and the suggested measures for Adobe. Where an indication of the timeline for measures to be taken by Adobe is available, the estimated timeframe is shown in bold.

[23] September 2025 Response to SURF Concerning Technical Mitigations (4 Oct 2025).

Table 1: Overview risks and suggested mitigating measures

No.	Risk	Measures
1.	Loss of control – Contractual framework	**Measures Educational Institutions**
		Agree on contractual purpose limitation. Explicitly define roles and responsibilities. Amend contract and DPA. Establish retention periods.
		Measures Adobe
		Establish a clear hierarchy between terms. Identify inconsistencies and harmonize terms. Amend contract and DPA. Establish retention periods. **The suggested measures will be part of the discussion in the context of the current contract renewal.**
2.	Loss of control – Role division	**Measures Educational Institutions**
		Explicitly define roles and responsibilities. Contractually limit the processing of Customer Data by Adobe. Include an exhaustive list of legitimate business purposes that clearly defines limitations on the categories of personal data processed, processing activities permitted, and retention periods for each purpose. Pay special attention to: - Product improvement and development - Statistics / anonymized information - To enforce its rights under this Agreement - General communication to users - Storage of content credentials - Fraud prevention, security, and misuse detection (including detection, review and reporting of illegal content) - Reporting illegal content. - legal compliance and responding to government requests.
		Measures Adobe
		Explicitly define roles and responsibilities.

		Present the controller with a detailed description of the service to enable the controller to define the purpose and the personal data processed for this purpose. **The suggested measures will be part of the discussion in the context of the current contract renewal.**
3.	Loss of Control - Adobe's use of Customer Data to enforce its rights	**Measures Educational Institutions**
		Restrict Adobe from using Customer Data for this broad purpose.
		Measures Adobe
		Do not use Customer Data for enforcing Adobe's rights. **The suggested measures will be part of the discussion in the context of the current contract renewal.**
4.	Lack of transparency – List of sub processors is incomplete	**Measures Educational Institutions**
		Exercise the audit right to regularly audit which subprocessors are used.
		Measures Adobe
		Provide transparency on the applicable subprocessors and maintain a complete list **(End of 2025)**.
5.	Loss of control - Not aware and thus not able to object to proposed changes sub processors	**Measures Educational Institutions**
		Ensure to sign up to receive the notifications.
		Measures Adobe
		Send the updates on subprocessors by default to the vendor compliance / purchase department.
6.	Loss of control – Adobe's cookies	**Measures Educational Institutions**
		Regularly audit the web traffic for not listed cookies.
		Measures Adobe
		Comply with the legal transparency requirements about cookies and similar technologies (improve explanation in Cookie Consent Manager and Cookie Policy). Implementing enhancements to the current scanning and review process **(Q1 2026).**
7.	Loss of control - Reporting to NCMEC	**Measures Educational Institutions**
		For use cases / school assignments involving content that could infringe Adobe's policies (such as certain art projects or creative assignments involving potentially controversial themes or nudity): - exclusively work in desktop applications, and

		- disable the use of cloud storage or only store files locally.
		Measures Adobe
		Perform an individual legitimate interest balancing test before each report to NCMEC.
8.	Disclosure of user data to foreign law enforcement by Adobe	**Measures Educational Institutions**
		For use cases / school assignments involving content that could infringe Adobe's policies (such as certain art projects or creative assignments involving potentially controversial themes or nudity): - exclusively work in desktop applications, and - disable the use of cloud storage or only store files locally.
		Measures Adobe
9.	Loss of control – File sharing by users	**Measures Educational Institutions**
		Encourage periodic review of which documents have been made public and implement manual removal procedures for public documents after a given period of time.
		Measures Adobe
		Provide clear messaging to users about which documents are shared publicly. **(End of 2026)** Provide prompts to users reminding them which documents are shared publicly. **(End of 2026)** Provide users the option to limit the amount of time a document is available publicly at the moment of sharing. Notify project creators when administrators change access rights over works
10.	Loss of control – Accessibility projects and files by administrators	**Measures Educational Institutions**
		Create internal policies wherein administrators notify creators of works when access rights have changed. Create internal policies that inform users who within an organisation can access their files at time of creation.
		Measures Adobe
		Notify project creators when administrators change access rights over works.

		Notify users when administrators access files and inform users that administrators can access files at the time of file creation.
11.	Loss of control – User is not aware that functionalities are offered by an online service	**Measures Educational Institutions**
		Clearly describe the key functionalities (including on-demand services).
		Measures Adobe
		Provide users with documentation and popups that inform them which functionality in desktop apps is offline, and which is shared with Adobe.
12.	Loss of control – Users restricted in the ability to delete documents	**Measures Educational Institutions**
		Inform users of the current technical limitations.
		Measures Adobe
		Allow users to 'Delete' items in the Creative Cloud web application in the same manner as the desktop application **(End of 2026).**
13.	Disproportionate processing of telemetry data	**Measures Educational Institutions**
		Opt out from optional telemetry when and where the option is made available.
		Measures Adobe
		Reduce the storage period of all telemetry Clarify what telemetry is considered mandatory, and what is considered optional Delete telemetry when user accounts are deleted Do not collect unnecessary telemetry, and define clearly what is necessary and what is not Publish and update a list of telemetry, clarify which is mandatory, and why. Additionally clarify which forms of telemetry are collected when the user has opted in. Do not collect telemetry from desktop application when used by students **(End of 2026)**.
14.	Loss of control – Content Credentials	**Measures Educational Institutions**
		-
		Measures Adobe
		Inform users about what is stored, for how long, for what purposes and who has access to that data (before they generate images). Do not store thumbnails, at least not for non-AI or partially AI content.

		Establish (not indefinite) retention periods for content credentials (especially for user IDs and thumbnails). Anonymize data after a certain period of time or delete it all together. Bring Content Credentials fully in line with the Code of Practice for AI Act article 50, when it comes into force in 2026.
15.	Inability to exercise data subject rights – incomplete DSAR responses Adobe	**Measures Educational Institutions**
		-
		Measures Adobe
		Provide complete data in the DSAR response. Provide complete descriptions / give sufficient context for the data subject to understand the returned data (for example explanations for internal codes). Continue to provide clear follow-up support to data subjects by answering any clarifying questions regarding their DSAR responses, ensuring they understand the information provided.
16.	Inability to exercise data subject rights – Administrators not able to honour DSARS	**Measures Educational Institutions**
		Create and maintain a dedicated process to handle DSARs from users.
		Measures Adobe
		Provide tooling for administrators to answer DSARs of data subjects. Provide clear guidance on system limitations. Ensure dedicated support from Adobe is available to assist administrators in navigating and completing DSAR requests.
17.	Inability to exercise data subject rights – Right to erasure / storage limitation	**Measures Educational Institutions**
		Create a clear work instruction around user deletion and user asset deletion. Ensure that users are removed from the 'Active users' lists after the user was removed. Use the Adobe Admin APIs for Storage Management to configure a retention policy for inactive users.
		Measures Adobe

		Simplify process of removing users, offering a way to remove a user and all of its directory entries **(End of 2026)**. Update documentation to match the reality of the deletion process **(End of 2026)**. Inform administrators explicitly that assets are kept when a user is deleted. Remove a user's assets along with the user account.

Introduction

This DPIA is commissioned by SURF, the collaborative organisation for IT in Dutch higher education and research.

Data Protection Impact Assessment

Under the terms of the General Data Protection Regulation (GDPR), an organisation may be obliged to carry out a data protection impact assessment (DPIA) under certain circumstances, for instance where it involves large-scale processing of personal data. 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.

A DPIA used to be called PIA, *privacy impact assessment*. According to the GDPR a DPIA assesses the risks for the rights and freedoms of individuals. 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 DPIA versus individual DPIAs

In GDPR terms SURF **is not the data controller** for the processing of personal data via the use of Adobe Creative Cloud and Adobe Document Cloud. The data controller is the individual education organisation that decides to use this cloud service. However, as central negotiator for many cloud services, 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 commissions umbrella DPIAs to assist the education organisations 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.

This umbrella DPIA is meant to help the different organisations with the DPIA they must conduct when they deploy Adobe Creative Cloud or Adobe Document Cloud, but this document cannot replace the specific risk assessments the different organisations must make themselves.

Criteria EDPB

Pursuant to article 35 of the GDPR, a DPIA is mandatory if an intended data processing constitutes a high risk for the data subjects whose personal data are being processed

The Dutch Data Protection Authority (Dutch DPA) has published a list of 17 types of processing for which a DPIA is always mandatory in the Netherlands.[24] If a processing is not included in this list, an organization must itself assess whether the data processing is likely to present a high risk.

The European national supervisory authorities united in the European Data Protection Board (EDPB) have also published a list of nine criteria.[6] As a rule of thumb if a data processing meets two of these criteria a DPIA is required.

The circumstances of the data processing via Adobe Creative Cloud and Adobe Document Cloud meet three 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. The processing involves data relating to vulnerable data subjects (criterion 7). Both employees and students whose personal data are processed through Adobe Creative Cloud and Adobe Document Cloud are in an unequal relationship of power with the education and research organisations.
3. The processing involves innovative use or applying new technological or organisational solutions (criterion 8). In case of Adobe Creative Cloud, the generative AI functionality offered by the Firefly cloud AI-services falls under this criterion.

Scope of this DPIA

Adobe Creative Cloud and Adobe Document Cloud are subject of this DPIA.

This DPIA for SURF includes the online Admin Console that allows an organization's administrator to manage licenses and settings for the organization when using both Adobe Creative Cloud and Adobe Document Cloud. In addition, the DPIA analyses the data protection risks of using the Photoshop (photo editing) Windows and MacOS creative applications. The analysis for this DPIA is extended to include a review of data processing through these services on macOS. Finally, Privacy Company also tested Adobe's generative AI functionality based on Firefly cloud AI-services. These functionalities are tested through the dedicated Firefly website, Photoshop and Adobe Express.

Table 2: Overview services and platforms in scope of this DPIA

	Web (Chrome)	Windows 11	macOS
Admin Console	x		
Acrobat Pro	x	x	x
Photoshop		x	x
Adobe Express Premium	x		

[24] Autoriteit Persoonsgegevens, URL: https://www.autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia.

Out of scope

The scope of this DPIA does not include the following:

- Acrobat AI Assistant[25]
- Rewrite and Translate text features.
- Adobe Sign[26]
- Adobe mobile apps
- Acrobat Microsoft Integrations (such as Microsoft SharePoint and OneDrive, Microsoft Teams, Microsoft Word, Excel, and PowerPoint).
- The 'legacy' Acrobat desktop application UI.[27]
- Beta features
- Adobe Collaboration Space, Adobe Developer, Adobe Fonts, Adobe Spark, Adobe Substance 3D, Adobe Behance, Adobe Demo Assets, Adobe Fuse, Adobe InDesign Server, Adobe Lightroom, Adobe Medium, Adobe Experience Cloud.
- Public webpages such as the Adobe Community forum (https://community.adobe.com/) and the Adobe Experience Cloud (https://experienceleague.adobe.com/).
- Aspects of Adobe's use of Amazon Web Services to host applications and content.
- Adobe Firefly IP Indemnification. Adobe Firefly IP Indemnification is only available in certain product offerings and must be included in the customer's contract to apply. SURF's current ETLA (Enterprise Terms Licensing Agreement) with Adobe does not include any of the aforementioned product offerings and thus lacks such a provision.[28]

Note: Content Credentials[29] are currently still a beta feature. However, since they are integrated in Firefly they are still included in this DPIA in a limited way. Adobe Stock is integrated in Firefly (as training data) and Adobe Stock is always present as service in the Adobe Creative Cloud (albeit in a limited way for K-12 users). Though Adobe Stock was out of scope as standalone service, accessing it via the Creative Cloud was tested.

This report is not a dedicated KIA[30], a Children's Rights Impact Assessment, but includes special sections focusing on children. It also does not include a separate IAMA, an Impact Analysis

[25] Acrobat AI Assistant can create summaries of or answer questions about PDF documents, based on natural language prompts from users. This product requires a separate license. Individual users can turn off generative AI features in the product settings and administrators can revoke access for the whole organization by contacting Adobe Customer Care. See: https://helpx.adobe.com/acrobat/using/disable-generative-ai.html, last viewed 6 January 2025. Also, email Adobe 17 January 2025: "This feature is available in beta in many locations and in several languages (English, French, Spanish, Portuguese, Italian, and German) and while AI Assistant can be purchased by customers in the Netherlands, it is not yet available in Dutch. It is also specifically restricted for EDU offerings (only being available to HED customers in specific countries). Users must always have to take a specific action to turn it on. It is also an ad on – meaning it costs more (though there may be limited trial options in certain circumstances). If you buy Adobe Acrobat Pro the AI is a separate line item. There may eventually be an offering for Enterprise customers (ETLA) in the future but not currently and to confirm AI Assistant is not something enterprise ETLA users can access by default either."

[26] Adobe Sign was initially part of the scope of the assignment. As Adobe Sign is a standalone product, a separate DPIA will be performed for Adobe Sign.

[27] In September 2024 Adobe made available a new Acrobat UI to all users. All our tests were performed while using this new UI. See 'Learn about the new Acrobat', last updated 16 September 2024, URL: https://helpx.adobe.com/acrobat/learn-new-acrobat.html.

[28] Email Adobe 19 January 2025.

[29] Adobe, 'Content Credentials', last updated 14 October 2024, URL: https://helpx.adobe.com/creative-cloud/help/content-credentials.html.

[30] Ministry of the Interior and Kingdom Relations, KIA Template, URL: https://www.digitaleoverheid.nl/document/kia-invuldocument/.

Algorithm and Human Rights when using built-in AI services. For this, the Ministry of the Interior and Kingdom Relations has developed a separate model.

Methodology

This DPIA is based on a comprehensive research methodology. Privacy Company combined a legal fact-finding strategy with a technical examination of the data processed through the use of Adobe Creative Cloud and Adobe Document Cloud.

Legal fact finding

Privacy Company has reviewed information provided by SURF and Adobe, as well as publicly available information. In addition, SURF, Adobe & Privacy Company had a workshop with Adobe's Trust & Safety team on Child Safety.

Technical examination

The technical part of the examination includes inspection of the settings available for administrators and end-users and performing test scenarios that aim to represent common use of the services.

Test scenarios

To ensure that all findings can be reproduced, Privacy Company performed scripted test scenarios. These scenarios are described in Section 2.3 and in the Technical Appendix. These tests cover typical uses cases for students and teachers on web-based Adobe Creative Cloud applications, Mac desktop Adobe Creative Cloud applications, and Windows desktop Adobe Creative Cloud applications. Privacy op School[31] provided feedback / input for the test scenarios. Privacy op School provided information about the regular (intended) use within primary and secondary education schools and to a lesser extent about the unintended or misuse of Adobe's products.

Technical Testing

Privacy Company used a combination of the tools Mitmproxy and Wireshark to intercept web traffic during the scripted test scenarios. These tools allow Privacy Company to observe cookies and other data types being sent from the test devices to outside servers. A summary of the test environment can be found in Table 3.

Table 3: Overview of technical tools used in testing

Tool	Version	Description of use
Windows laptop	Processor: 11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz 2.30 GHz, x64-based processor Microsoft Windows 11 Pro	Used when intercepting traffic and to run Adobe Applications.
Mac laptop and Google Chrome browser	macOS 10.15.7 Apple M3 Pro processor Google Chrome[32] browser version 129	Used when intercepting traffic and to run Adobe Applications on desktop and web.

[31] Privacy at School is a Dutch organisation that aims to help and support all organisations in education with privacy and information security issues URL: https://www.privacyopschool.nl/.

[32] Google, Chrome, URL: https://www.google.com/chrome/, last viewed 4 February 2025.

Mitmproxy	Version 10.2.4[33]	Used to intercept web traffic from browser and Adobe applications.
Wireshark	Version 4.0.7[34]	Used to intercept web traffic from browser and Adobe applications.
Adobe Creative Cloud Desktop Application[35]	Version 6.4.0.361	Used to run the test scenarios.

Outline of this DPIA

This DPIA follows the structure of the Model Gegevensbeschermingseffectbeoordeling Rijksdienst (DPIA). This model 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 Adobe Creative Cloud and Adobe Document Cloud in detail in general terms, based on the tested setup. This starts with a description of the way the data are collected and processed and describes the categories of personal data and data subjects that may be affected by the processing, the purposes of the data processing, the different roles of the parties, the different interests related to this processing, the locations where the data are stored and the retention periods. For this part, SURF's contract with Adobe, as well as other legal documentation has been reviewed. In addition, test scenarios were executed, and data subject access requests were filed, and additional information was requested from Adobe.

Part B provides an assessment by Privacy Company of the lawfulness of these data processing operations through Adobe Creative Cloud and Adobe Document Cloud. Privacy Company has assessed compliance with the key principles of data processing, starting with the legal ground, and including transparency, data minimisation, purpose limitation, and proportionality. This section also separately addresses the legitimacy of any transfers of personal data to countries outside of the EEA, as well as how the rights of the data subjects are respected.

Part C assesses the risks to the rights and freedoms of the data subjects created by the processing activities resulting from the use of Adobe Creative Cloud and Adobe Document Cloud in Part A of this DPIA. It names specific risks that derive from these processing operations 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. Part C also contains an analysis of the severity of each risk, based on the likelihood of its occurrence and potential impact on the rights and freedoms of data subjects.

[33] Mitmproxy, HTTPS proxy., URL: https://mitmproxy.org. last viewed 20 December 2024.

[34] Wireshark, network protocol analyser, URL: https://www.wireshark.org/, last viewed 20 December 2024.

[35] Adobe Creative Cloud, URL: https://creativecloud.adobe.com/, last viewed 20 December 2024.

Finally, **Part D** outlines concrete measures that can be implemented either by Adobe or the educational institutions to mitigate the risks identified in Part C. These measures might reduce the likelihood of those risks occurring, their potential impact, or both. Part D also contains an assessment of any residual risk associated with the use of Adobe Creative Cloud and Adobe Document Cloud to the extent they cannot be mitigated by the educational institutions by applying the suggested measures.

Timeline of this DPIA

This timeline is based upon correspondence between Privacy Company, SURF, and Adobe throughout the project. While the timeline is factual, it does not capture any direct communications or exchanges that may have occurred between SURF and Adobe.

Several early meetings and scoping discussions took place before formal fact-finding began. For clarity, this timeline starts from the point when Privacy Company began technical testing. The technical testing took place in weeks 37, 38, and 39 of 2024. The DSARs were submitted on 30 September 2024 and Adobe confirmed the receipt of the DSARs on 3 October 2024. Adobe provided an initial personal data response on 30 October 2024, followed by a more comprehensive response with additional information on 13 December 2024. The second response was the more detailed return of data, which had been indicated would require additional time.

The first draft of Part A of this report was completed on 7 February 2025. Part A reflects a point in time analysis of Adobe software and services prior to Adobe responding to SURF's observations with clarifications, corrections, changes, or planned. mitigations. Where Adobe has undertaken such work, it is addressed by SURF at the end of the descriptions in Part A. As such, the descriptions of Part A should not be understood as current state [date of publication of this DPIA], but rather as an initial analysis, prior to the collaborative work undertaken by Adobe and SURF. Where work has been done, or issues clarified, SURF has noted this at the end of the section to reflect the starting point and now current state.

On 14 May 2025 the full draft of the DPIA was completed. Throughout 2025, several rounds of questions and feedback were undertaken on the report, including clarification of issues and working towards solutions. On 22 September 2025, Adobe, SURF and Privacy Company had a meeting to discuss Adobe’s Trust and Safety measures, including its CSAM scanning methods and techniques.

The final report was completed on 12 February 2026.

Part. A Description of the 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 processed personal data, and the processing purposes. In addition, Part A provides an overview of the personal data processed, the parties involved, the interests of the parties involved in the processing, and the techniques and methods of data processing. Also covered are the legal and policy framework and retention periods.

1 The processing of personal data

This section starts with an introduction of Adobe Creative Cloud and Document Cloud in Sections 1.1 and 1.2. Section 1.3 describes the admin console and briefly introduces identity types. Section 1.4 covers Adobe Cloud Storage. The contractual framework as relevant to SURF members is set out in Section 1.5. The section ends with addressing Child Safety in Section 1.6.

1.1 Creative Cloud

Adobe Creative Cloud gives users access to a collection of software developed by Adobe for graphic design, video editing, web development, photography, and cloud services.[36] Adobe Creative Cloud includes Adobe Acrobat Pro and can be deployed as on-premise software and on-demand services. On-premise applications are primarily installed and operated on a user's local infrastructure. On-demand services are additional features hosted on the cloud storage side. There is no publicly available information that distinguishes the features that are included in the on-premise applications from those that are available as additional on-demand options.

The General Terms[37] that are part of the Enterprise Licensing Terms[38] (see also Section 1.5.1.2) describe on-premise software as *"the Adobe software that is deployed by or on behalf of Customer on hardware designated by Customer".*[39] On-demand services are described as *"the technology services hosted by or on behalf of Adobe and provide to Customer as a shared instance".*[40] In addition to this the Terms also give a definition for Managed Services: *"the technology services hosted by or on behalf of Adobe and provided to Customer as a dedicated instance".*[41] These definitions are relevant for the applicability of the Data Processing Agreement (DPA), see also Section 1.5.1.2.

[36] Adobe Creative Cloud | Product description, URL: https://helpx.adobe.com/legal/product-descriptions/creative-cloud.html#main-pars_text_1, last updated 19 October 2019.

[37] Adobe General Terms (2024v1), URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf/

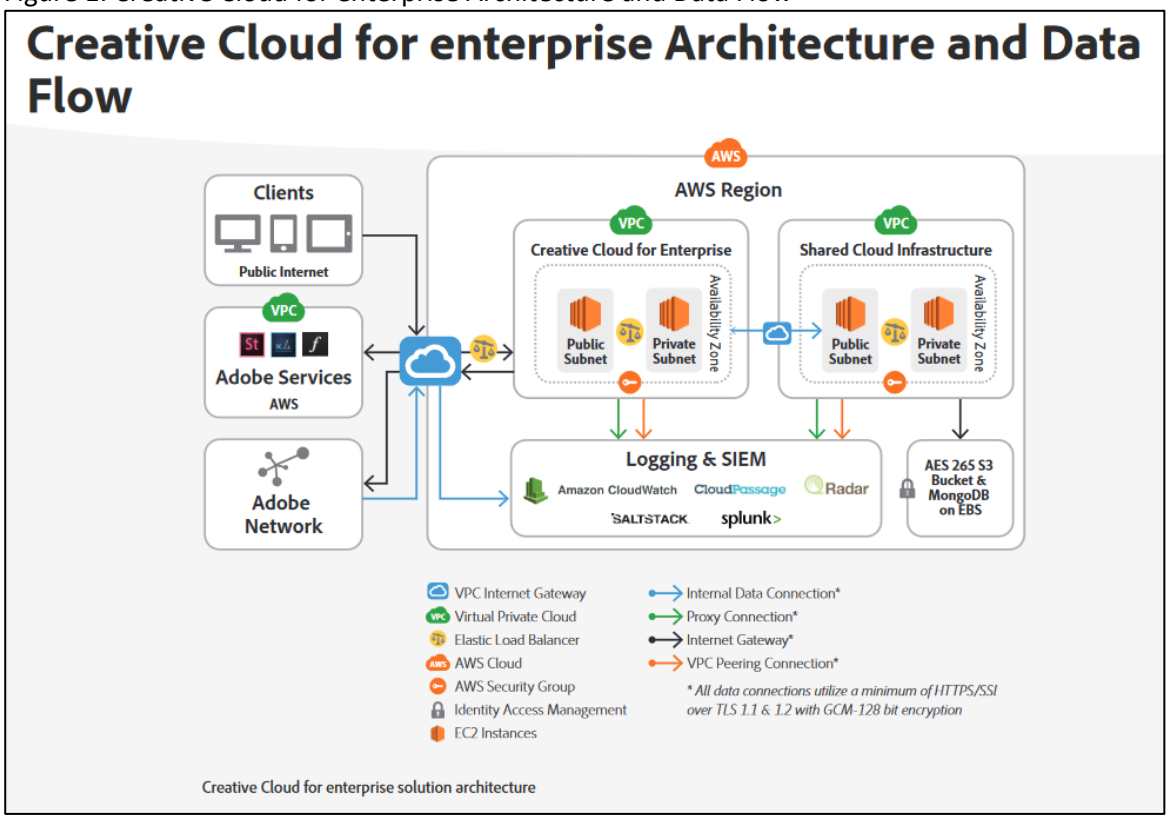
[38] "Available at http://www.adobe.com/legal/terms/enterprise-licensing.html".

[39] Article 1.24 Adobe General Terms (2024v1).

[40] Article 1.23 Adobe General Terms (2024v1).

[41] Article 1.22 Adobe General Terms (2024v1).

Figure 1: Creative Cloud for enterprise Architecture and Data Flow[42]



Admins of an enterprise organization can configure services and storage availability for groups of users from within the Adobe Admin Console. Both Creative Cloud for enterprise and Document Cloud for enterprise plans include services that can be configured. See also Sections 1.3 and 3.1.

Certain services are not displayed in the Admin Console. These services are core to the product function and are always on with a plan that includes storage. Core services are not configurable (also see Section 3.1.3.2).[43]

PDF Services enable certain PDF operations in Acrobat that require data processing in Adobe Cloud and include a set of services that allow validated users access to web applications.[44] These services and applications are accessed from a customer system through four endpoints:

- Desktop applications such as Acrobat Reader DC, Acrobat Pro DC, or Acrobat Standard
- Mobile applications (out of scope)
- A web browser
- Acrobat in Microsoft 365, such as Teams or Office (out of scope)

[42] Adobe, Whitepaper, Creative Cloud for enterprise, Security Overview, October 2021, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/cce_security_whitepaper.pdf.

[43] Adobe, 'Enable/disable services for a product profile', last updated 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/enable-disable-services.html.

[44] Adobe, 'Enable/disable services for a product profile', last updated 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/enable-disable-services.html.

PDF Services are essential tools to store and share files online and work across surfaces and support the following features:

- Share for Review
- Storage Integrations
- Editing and multi-user commenting in Microsoft Teams (out of scope)
- Compare
- Liquid Mode on Mobile (out of scope)
- Manipulate documents in Adobe Scan app (out of scope)

Creative Cloud for Education

Adobe offers several Creative Cloud plans for Education: Creative Cloud for Students and Teachers, Creative Cloud for K12/Primary and Secondary Schools (K-12), and Creative Cloud for Higher Education Institutions (HED).

The K-12 plan is typically offered to primary education schools and educational institutions catering to younger children while the HED plan is aimed at colleges and universities (and older students). These two plans also come with different features and controls. HED users have potential access to the additional Adobe products Behance and Portfolio (which allow for easy sharing and distribution of content online). HED users can also opt in to marketing, whereas a K-12 end user is restricted by default from being able to opt-in to marketing. There are also certain content filters applied by default to K-12 licenses (e.g., certain images not being able to be accessed in Adobe Stock).[45] K-12 students use school-managed Enterprise/Federated IDs, while HED students can have an Adobe ID account. 'Domain enforcement' is available on customer domains, disallowing creation of Adobe IDs.[46] See also Section 3.1.2.4.

The differences between the K-12 and HED plans are outlined in the Adobe Student Privacy Notice, which is available online.[47] In addition to this Privacy Notice, Adobe offers the K-12 (Primary and Secondary) and Higher Education Product Specific Terms for Student Data.[48] This document is described in Section 1.5.1.3.

Adobe pointed out that *"for enterprise accounts purchased by an educational institution, the educational institution retains significant control over any personal information processed as part of providing the products and services (e.g. schools can choose to identify students by aliases rather than their emails or student ID numbers)."*[49] In order for students to have the extra safeguards the system administrator must identify users as the correct type (K-12 student, HED student or staff member) in the admin console, according to Adobe. It is not clear how to set up this particular configuration, see more about this in Section 3.1.

[45] DSAR Response of 30 Oct 2024, p. 2 and 3.

[46] Adobe, Domain Enforcement for restricted authentication, last updated on Dec 16, 2024, URL: https://helpx.adobe.com/enterprise/using/restricting-domains.html.

[47] Adobe & Student Privacy, Last Updated 21 July 2021, URL: https://www.adobe.com/privacy/student-policy.html.

[48] K-12 (Primary and Secondary) and Higher Education Product Specific Terms for Student Data, last updated June 18, 2024, URL: https://wwwimages2.adobe.com/content/dam/cc/en/legal/servicetou/Adobe-EDU-Terms-en_US-20240618.pdf.

[49] DSAR Response of 30 Oct 2024, p. 3.

1.2 Document Cloud

Adobe Document Cloud is a cloud-based suite of tools and services for managing and working with digital documents, particularly PDFs. Adobe Acrobat is the core software within Document Cloud. Users can create, view, edit, and convert PDFs and the suite includes tools for sharing documents with others, adding comments or annotations, and tracking changes. Document Cloud includes Adobe Sign & Fill, allowing users to fill out forms and add their own signatures to PDF documents.[50] Document Cloud also provides cloud storage for PDFs and other document types.

The Adobe Acrobat Pro software can be used as a mobile application, as a desktop application and as a Web application, via the browser. Privacy Company performed its test scenarios with a Chrome browser. Mobile apps are out of scope of this DPIA.

Adobe Document Cloud services include the following[51]:

- Send PDF — Send a PDF to a recipient using an email client
- Organize PDF — Insert, delete, reorder, or rotate pages in a PDF
- Create PDF — Convert Word, Excel, and PowerPoint documents, as well as images or
- photos, into PDF files
- Export PDF — Convert PDFs into editable Microsoft Word, Excel, PowerPoint, or RTF files
- Edit PDF — Edit existing PDFs from a mobile device or laptop
- Combine PDF — Combine multiple files into a single PDF and assemble document packages from anywhere
- Fill & Sign — Complete a form and add a signature
- Adobe Scan — Capture and convert anything into a searchable, high-quality PDF

With Document Cloud services, users can also use the certificates tool, which enables users to sign documents with an e-signature backed by a digital certificate that is cryptographically bound to the signature field. Each digital certificate (or digital ID) uniquely identifies the signer and is issued by a trust service provider (TSP) or certificate authority (CA) listed on the Adobe Approved Trust List (AATL) or the European Union Trusted Lists (EUTL). The Certificates tool also allows users to add timestamps to documents and certify documents with a tamper-evident seal. [52]

Adobe has also integrated Acrobat into several Microsoft productivity tools. The behaviour of document storage for these integrations is different from standalone Acrobat. These integrations are out of scope of this DPIA.

1.3 Admin Console

The Adobe Admin Console is used to manage user accounts as well as to configure license and service entitlements. It provides role-based access to Creative Cloud for enterprise apps and services and enables user management and entitlement access to Adobe Document

[50] The DPIA may describe what data QuoVadis receives from Adobe but does not examine the processing performed by QuoVadis.

[51] Adobe, Adobe Acrobat with Document Cloud Services Security Overview, p. 4, February 2024, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/doc-cloud/acrobat-dc-security-overview-ue.pdf.

[52] Adobe, Adobe Acrobat with Document Cloud Services Security Overview, p. 8, February 2024, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/doc-cloud/acrobat-dc-security-overview-ue.pdf.

Cloud, Adobe Marketing Cloud (out of scope), and Print & Publishing applications (out of scope). IT staff can also utilize the Admin Console to open support cases with Adobe Customer Care or schedule Expert Services sessions.[53]

1.3.1 Identity Types

Adobe's identity management system enables admins to create and manage user's access to applications and services. There are three different identity types on Adobe Admin Console: (1) Federated ID, (2) Enterprise ID, and (3) Adobe ID. The identity types allow an organisation different levels of control over the users' accounts and data. The choice of identity model has a "*considerable impact on how the organization stores and shares assets*". Federated and Enterprise ID models are created and managed by the organisation (see Section 3.1.2).[54] The organisation manages user-credentials and uses Single Sign-On (SSO) via a SAML2 identity provider (IdP) for Federated IDs. The Enterprise ID enables the organization to retain exclusive rights to create user accounts on verified domains. Adobe IDs are created, owned, and managed by the end user. Adobe performs the authentication, and the end user manages the identity. Depending on the storage model, users or businesses retain control over files and data.[55]

1.4 Adobe Cloud Storage

Adobe Cloud Storage is the storage for Adobe Creative Cloud and Adobe Document Cloud. For Document Cloud, it only includes Adobe Acrobat and PDF Services.[56] Admins can set up organisation-wide security and compliance parameters for cloud services available in their own region.

Adobe Cloud Storage is hosted on Amazon Web Services (AWS) in data centres at North America, EMEA, and Japan. The EMEA data centre is located in Dublin, Ireland.[57] When hosted by Amazon Web Services (AWS), customer transaction data, documents, and metadata are stored in Amazon Simple Storage Service (S3) and Elastic Block Store (EBS).[58]

Adobe Cloud Storage cannot be disabled by administrators as it is an *'always on'*-service[59] (see Section 3.1.3.2) and the Enterprise Storage Model does not provide a mechanism to prohibit cloud data storage (see Section 3.1.5).[60]

---

[53] Adobe, Whitepaper, Creative Cloud for enterprise, Security Overview, October 2021, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/cce_security_whitepaper.pdf.

[54] Adobe, 'Identity overview', URL: https://helpx.adobe.com/enterprise/using/identity.html, last visited 26 October 2024.

[55] Idem.

[56] Adobe, Adobe cloud storage data centers, 'To which solutions in the Adobe Document Cloud does it apply?', URL: https://helpx.adobe.com/document-cloud/help/adobe-cloud-storage-datacenters.html, last viewed 15 November 2024.

[57] Adobe, Adobe cloud storage data centers, last updated on 10 December 2024, URL: https://helpx.adobe.com/document-cloud/help/adobe-cloud-storage-datacenters.html.

[58] Adobe, Adobe cloud storage data centers, last updated on 29 June 2023, URL: https://helpx.adobe.com/document-cloud/help/adobe-cloud-storage-datacenters.html.

[59] Adobe states: *"Certain services are not displayed in the Adobe Admin Console, are core to the product function, and are always on with a plan that includes storage. Core services are not configurable."* in Enable/disable services for a product profile, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/enable-disable-services.html.

[60] Creative Cloud for enterprise Security Overview, October 2021, p. 5. Adobe has stated in an email to SURF of 28 March 2025 that the inability to disable cloud storage *"is true of certain applications such as Adobe Express, which rely on foundational core services including*

Any Adobe customer that owns school/enterprise entitlements under a contract is provisioned as a separate tenant. This means that all contracted education and government customers have their own tenant. Essentially, every customer has their own independent tenant.[61]

1.5 Contractual framework

This section outlines the legal documentation. Section 1.5.1 covers Adobe Creative Cloud for Education **as contracted through SURF** and Section 1.5.2 focuses on Adobe Document Cloud. Section 1.5.3 includes general legal documents such as Adobe's Terms of Use, Privacy Policy, and Cookie Policy.[62]

1.5.1 Creative Cloud for Education – SURF and Consortium

SURF ('Consortium') has entered into an Enterprise Term License Agreement (ETLA) with Adobe. There is a participation agreement with a digital signature process for each SURF member ('Consortium Member') that participates under the Adobe contract, which arranges how the SURF member relates to the agreement. Each SURF member signs their own DPA with Adobe, which is available through Adobe's Self Service Portal.[63]

The agreement (hereinafter: 'Agreement') between SURF and Adobe consists of:

- The Sales Order[64]
- The parts of the Adobe Enterprise Licensing terms[65], consisting of:
    - The General Terms, and
    - The applicable Product Specific Licensing Terms *"which are effective as of the date Customer executes this Sales Order."*

1.5.1.1 Sales Order

The Sales Order lists the Products and Services included in the Agreement. These Products and Services are listed in two tables and divided by Adobe On-demand services, and Creative Cloud, Document Cloud and Software. The Adobe Creative Cloud, Document Cloud and Software table is essentially comprised of "on-premise" applications that are primarily installed and operated on a user's local infrastructure with access to additional features hosted on the cloud storage side (which can be distinguished from the "on-premise" side by instead being connected "on-demand" components). Accordingly, the on-demand table includes products that are purely "on-demand" rather than "on-premise".[66]

Cloud Storage. For certain applications (other than Adobe Express), where Cloud Storage is not needed for a foundational core service, Admins can configure applications through the Admin Console to avoid using Cloud Storage. When Admins do so, users will be unable to create Cloud documents." Privacy Company has revisited the Admin Console but was not able to locate a setting to disable cloud storage.

[61] Email Adobe to SURF 7 June 2024.

[62] SURF, SLB and APS are co-operating generally in matters dealing with the Dutch education sector. Adobe has engaged with each party to jointly discuss the business relationship and foster greater collaboration between the parties for the advancement and benefit of the education sector in The Netherlands. Each of the three organisations has its own ETLA with Adobe. SURF's ETLA is reviewed for the purpose of this DPIA.

[63] Email SURF 21 June 2024.

[64] Adobe Contract Number: 00818261.

[65] "Available at http://www.adobe.com/legal/terms/enterprise-licensing.html".

[66] Email Adobe 13 December 2024.

According to the Agreement between SURF and Adobe, SURF must enter into a sales order with each Consortium Member[67] in the format provided as Exhibit A to the Consortium Sales Order and must provide Adobe with a copy of such Consortium Sales Order upon request.

As with SURF's Agreement with Adobe, the Consortium Member Enterprise Term License Sales Order, the reseller agreement share the same terms and structure (Sales Order, General Terms, and Product Specific Licensing Terms). *"Adobe is an intended third party beneficiary of this Agreement between Consortium and Consortium Member and has a right to enforce its terms against Consortium Member. Consortium Member will be deemed a "Customer" as such term is used in Adobe Enterprise Licensing Terms"*.[68]

The Agreement explicitly mentions that Consortium Members may only deploy the offering for primary and secondary school students using Enterprise and Federated IDs (see Section 1.3.1). The deployment of Enterprise or Federated IDs is essential to ensuring Adobe can meet its student privacy commitments to Consortium Member and that Adobe does not track or market to Student users. Use of Enterprise or Federated IDs also ensures Consortium Member retains control over the applications and services available to K-12 Students and the files and data K-12 Students store. *"Any assignment of an individual Adobe ID to a K-12 Student nullifies any representation or warranty Adobe makes regarding the use and protection of K-12 Student data, and Consortium Member must defend and indemnify Adobe for any Student privacy or other claims related to Consortium Member's license deployment using an Adobe ID for the Offering"*[69] For HED students, educational institutions can also work with Adobe IDs (see also Section 1.3.1).

The Agreement includes clauses about FERPA (Family Educational Rights and Privacy Act) and COPPA (Children's Online Privacy Protection Act) compliance, and special terms *for "other jurisdictions"* (See also Section 9.4). The provision refers to laws that require Consortium Members to:

- Provide disclosures to parents regarding the collection of Student personal information for K-12 students;
- Obtain parental consent, including verifiable consent from parents regarding cross-border data transfers[70];
- Provide disclosures to and obtain consent from parents regarding content ownership, or include a link to Adobe's Privacy Policy in any parent notification or consent request Consortium Member provides.

The Agreement states that Adobe is Consortium Member's data processor and the Consortium Member is the data controller in connection with the collection of Student personal data *"in the Offering and in an other Adobe application that Consortium Member allows K-12 Students to access"*.[71] For further details about how Adobe collects, uses, and discloses personal data collected from Students the Agreement refers to Adobe's Privacy Policy. This is unusual and

[67] 'Consortium Member' means that educational institution that meets the education eligibility criteria for Adobe's education programs.

[68] Consortium Member Enterprise Term License Sales Order, Article 17.

[69] Consortium Member Enterprise Term License Sales Order, Article 20.1.

[70] Adobe clarified in its response to Draft A of this DPIA, that consent is the legal bases, *"if required in the applicable jurisdiction. As per our contracts, the Controller would be responsible for the legal basis for this category of data."*

[71] Consortium Member Enterprise Term License Sales Order, Article 20.2 and 20.3.

confusing, as the privacy policy outlines how Adobe processes personal data as a controller, rather than as a processor.

In response to the first draft of Part A Adobe clarified: *"Adobe's position has always been that in terms of data processing as between its customers and Adobe, the details are set out in the agreements themselves. As stated here we only point to the Adobe Privacy Policy for "further details"- when it comes to processing as a processor, the Data Processing Agreement together with the General Terms is instructive."*

Neither SURF's Agreement with Adobe, nor the draft Consortium's Member Agreement includes any explicit reference to a DPA or to the specific Student Data Terms. The General Terms (referenced in Article 17 of the Consortium Member Agreement) that are a part of Adobe's Enterprise Licensing Terms do mention the DPA *"and is incorporated by reference, except where explicitly agreed otherwise between the Parties"*.[72] Adobe explained that the reference to *"agreed as otherwise"* allows SURF consortium members to use Adobe's DPA Self-Service portal to generate a separate DPA themselves (which was explicitly discussed and agreed previously with SURF).[73] According to Adobe, the Student Data Terms are included by reference, since Article 1.16 of Adobe's General Terms include them in the definition "Documentation". However, as the article is broadly worded it is not evident that it extends to the Student Data Terms.

The relevant clauses from the DPA that is available via Adobe's website "Data Processing Addendum (Cloud Services Only)"[74] are mentioned throughout this DPIA.

1.5.1.2 Adobe Enterprise Licensing terms

The Sales Order references the applicable Adobe Enterprise Licensing Terms via a hyperlink.[75] The Adobe Enterprise Licensing terms[76] consist of:

- The General Terms[77], and
- The applicable Product Specific Licensing Terms (PSLT)

The following PSLT are relevant for this DPIA[78]:

- PSLT for Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1). [79]

---

[72] Article 1.14d Adobe General Terms (2024v1), (2024v1), Effective Date: 8 March 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf.

[73] Email Adobe 28 March 2025.

[74] Adobe Data Processing Addendum (Cloud Services Only), June 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/DPA-WW.pdf.

[75] Adobe, Enterprise Licensing Hub, URL: https://www.adobe.com/legal/terms/enterprise-licensing.html.

[76] "Available at http://www.adobe.com/legal/terms/enterprise-licensing.html".

[77] Adobe General Terms (2024v1), (2024v1), Effective Date: 8 March 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf.

[78] Email Adobe 13 December 2024. The PSLT for Acrobat Sign are also applicable for SURF's Sales Order. Acrobat Sign will be assessed in a separate DPIA.

[79] Adobe, PSLT – Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1), URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-CreativeCloudandDocumentCloudSubstance3D-WW-2023v1.pdf.

- PSLT for Adobe Desktop Software (2019v1).[80]
- PSLT for Stock (2024v1).[81]

For Firefly (Generative AI) the PSLT for Creative Cloud and Document Cloud and the Firefly Product description apply (see also Section 8.1.3).[82]

To the extent of any conflict or inconsistency, the following order of precedence will apply: the Sales Order, the Data Processing Addendum, the applicable Product Specific Licensing Terms, followed by the General Terms (Adobe's Enterprise Licensing Terms).[83]

The General Terms include definitions, clauses on payment of fees, delivery, license and restrictions, third-party access, confidentiality, indemnities, limitation of liability, warranties, license compliance, professional services, term and termination, and general provisions. A clause is dedicated to Customer data. It describes the ownership, permitted use, responsibility, data retention and usage information, and includes terms about Consumer generated content uploaded to the Cloud. Permitted use is described in Section 4.1.1. There is no clause about prohibited use of personal data by Adobe in these General Terms.

The General Terms and PSLT that are part of the Enterprise Licensing Terms apply to enterprise users. However, similarly named documents also exist for end-users, which can create confusion about which terms apply in a given context.

1.5.1.3 K-12 and Higher Education Product Specific Terms for Student Data

The 'K-12 (Primary and Secondary) and Higher Education Product Specific Terms for Student Data'[84] (hereinafter Student Data Terms) are entered into between Adobe and the educational institution ("Customer"), and govern the privacy of Student Data provided to Adobe by users during the use and deployment of Adobe products and services (the "Services") to students enrolled at qualified schools in K-12 (primary and secondary school) or higher education environment. The Student Data Terms govern the use of the service along with Adobe's General Terms of Use (TOU). Note that the Student Data Terms link to Adobe's General Terms of Use, not the General Terms that are part of the Enterprise Licensing Terms.

If there is any conflict between the terms in the General Terms and the Product Specific Terms (in this case the Student Data Terms), then the Product Specific Terms govern in relation to those Services or Software.[85] The Student Data Terms also take precedence over Adobe's Privacy

[80] Adobe, PSLT – Adobe Desktop Software (2019v1), https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-DesktopSoftware-2019v1-WW.pdf.

[81] Adobe, PSLT – Adobe Stock (2024v1), URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-Stock-WW-2024v1.pdf.

[82] Email Adobe 13 December 2024.

[83] Article 14.9, Adobe General Terms (2024v1), Effective Date: 8 March 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf.

[84] K-12 (Primary and Secondary) and Higher Education Product Specific Terms for Student Data, Last updated June 18, 2024, URL: https://wwwimages2.adobe.com/content/dam/cc/en/legal/servicetou/Adobe-EDU-Terms-en_US-20240618.pdf.

[85] Article 1.2 'Product Specific Terms, Adobe General Terms of Use, Effective as of 18 June 2024, URL: https://www.adobe.com/legal/terms.html.

Policy.[86] There is no clause establishing the hierarchy between the Student Data terms and the DPA published on Adobe's website. Adobe's Enterprise Licensing Terms, its General Terms, and Specific Product Licensing Terms are not mentioned in the Student Data Terms.

The use of Enterprise IDs or Federated IDs is *"essential for Adobe to meet its Student privacy commitments to Customer*". Any deployment of an individual Adobe ID (see Section 1.3.1) to a user nullifies any commitment Adobe makes regarding the use and protection of Student Data.[87]

Furthermore, personal data collected from Student Adobe IDs would be subject to the Adobe Privacy Policy, as modified by the further limitations in the Adobe EDU Terms together with the Data Processing contractual terms in place (which would apply to a customer in the Netherlands). These additional terms essentially limit Adobe's uses of personal data for aspects like marketing.[88]

1.5.2 Document Cloud

Section 1.5.1.2 outlines the General Terms and the Product Licensing Terms for Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1),[89] which also applies to Adobe Document Cloud.

1.5.3 Adobe's general legal documentation

Throughout the documentation references are made to Adobe's General Terms of Use (TOU) and Adobe's Privacy Policy. For that reason, these documents are covered in this section. This section finishes with Adobe's Cookie Statement.

1.5.3.1 Adobe's General Terms of Use.

Adobe's General Terms of Use (TOU) along with any of the 22 additional applicable Product Specific Terms govern the use of and access to Adobe's websites, web-based applications and products, customer support, discussion forums or other interactive areas or services, and services such as Creative Cloud and the installation and use of any software that Adobe includes as part of the Services. If a customer has entered into another agreement with Adobe concerning specific Services and Software, then the terms of that agreement control where it conflicts with the Terms. The Enterprise Licensing Terms would therefore take precedence of the TOU.

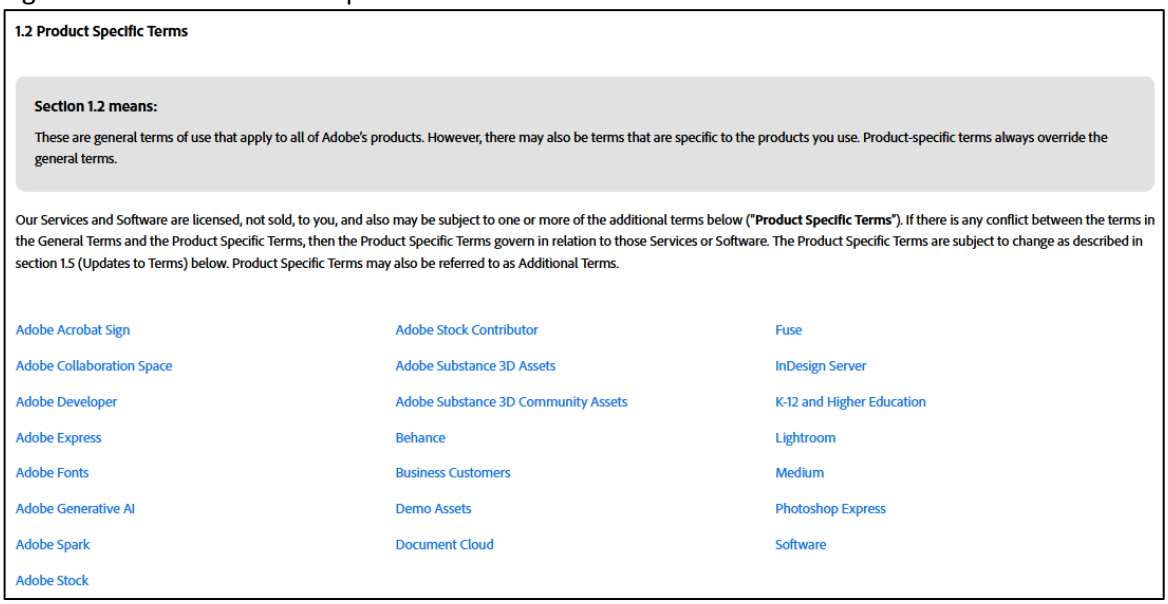
[86] Preamble of the K-12 (Primary and Secondary) and Higher Education Product Specific Terms for Student Data, Last updated June 18, 2024, URL: https://wwwimages2.adobe.com/content/dam/cc/en/legal/servicetou/Adobe-EDU-Terms-en_US-20240618.pdf.

[87] Article 2.1 Student Data Terms.

[88] DSAR response page 6.

[89] Adobe, PSLT – Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1), URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-CreativeCloudandDocumentCloudSubstance3D-WW-2023v1.pdf.

Figure 2: Overview Product Specific Terms



1.2 Product Specific Terms

Section 1.2 means:

These are general terms of use that apply to all of Adobe's products. However, there may also be terms that are specific to the products you use. Product-specific terms always override the general terms.

Our Services and Software are licensed, not sold, to you, and also may be subject to one or more of the additional terms below ("**Product Specific Terms**"). If there is any conflict between the terms in the General Terms and the Product Specific Terms, then the Product Specific Terms govern in relation to those Services or Software. The Product Specific Terms are subject to change as described in section 1.5 (Updates to Terms) below. Product Specific Terms may also be referred to as Additional Terms.

Adobe Acrobat Sign	Adobe Stock Contributor	Fuse
Adobe Collaboration Space	Adobe Substance 3D Assets	InDesign Server
Adobe Developer	Adobe Substance 3D Community Assets	K-12 and Higher Education
Adobe Express	Behance	Lightroom
Adobe Fonts	Business Customers	Medium
Adobe Generative AI	Demo Assets	Photoshop Express
Adobe Spark	Document Cloud	Software
Adobe Stock		

For the purpose of this DPIA, the following additional terms were reviewed: Adobe Express, Adobe Generative AI, Adobe Stock, Business Customers, Document Cloud, K-12 and Higher Education ('Student Data Terms'), Photoshop Express, and Software.

1.5.3.2 Adobe's Privacy Policy

The Adobe Privacy Policy describes the privacy practices of Adobe's Services and Software (as defined in Adobe's General Terms of Use) and anywhere Adobe displays or references the Privacy Policy.

The Privacy Policy describes how Adobe uses the user's personal data in the context of:

- Adobe websites; web-based services such as Behance; and web-based aspects of the Creative Cloud, Document Cloud and Experience Cloud;
- Services that display or include a reference to the Privacy Policy;
- Adobe's marketing, sales, and advertising practices; and
- *"The privacy practices of previously acquired companies, unless otherwise noted here".* [90]

There is an extra webpage with privacy information for Adobe Acrobat.[91]

1.5.3.3 Adobe's cookie statement

Adobe's Cookie statement[92] provides only a general overview of what cookies, similar technologies, and web beacons are. It mentions a few purposes for the use of the cookies by Adobe and *"the companies that help us run our business"*, but the explanations are very general and lack detailed specifics. Information about the types of cookies used (e.g. functional, analytics) for what purpose, the use of the data, and data retention practices are not included in the cookie statement.

---

[90] Adobe Privacy Policy, 'What does this privacy policy cover?', last updated 18 June 2024, URL: https://www.adobe.com/privacy/policy.html#cover.

[91] Adobe Acrobat, last updated: 4 May 2022, URL: https://www.adobe.com/privacy/policies/adobe-acrobat.html.

[92] Adobe, Cookies and Similar Technologies, last updated: December 5, 2022, URL: https://www.adobe.com/privacy/cookies.html.

Specific information about the cookies is provided through the cookie consent manager, which is available via the cookie banner and the "Cookie Preferences" link at the bottom of the Adobe webpage. Section 3.2.1 describes the cookie banner in more detail.

1.6 Child Safety

Child sexualisation, exploitation, and abuse material is not permitted on Adobe's products or services. Adobe has a zero-tolerance policy against any content uploaded to Adobe's servers that sexualises, endangers, or otherwise depicts the abuse of children. Adobe also prohibits child nudity in some instances where Adobe believes there is a high potential for abuse by others.[93]

The policy on 'Harmful Content' states that all prohibited content that is shared will be removed.[94] Uploading child sexualisation, exploitation, and abuse material to private storage will result in account termination. Prohibited content uploaded to private storage that does not meet the legal definition of child pornography will not be individually removed but may result in account termination.

The policy describes content that sexualises, exploits, or depicts the abuse of minors and lacks literary, artistic, political, or scientific value, and lists the rules when it comes to child nudity. Adobe does not prohibit all content that contains child nudity but does prohibit sharing the following content containing child nudity if there is:

- Visible genitalia or pubic area even if fully or partially covered by transparent clothing or visible by impression through tight clothing
- Visible anus even if fully or partially covered by transparent clothing or visible by impression through tight clothing
- Uncovered female nipples for children older than toddler-age
- Accidental exposure of portions of breasts, genitalia, or buttocks (for example, clothing falling or draping down to expose the minor)

The only exceptions for non-sexualized child nudity are:

- Content with artistic and/or historic significance that is generally recognizable globally (for example, the "Napalm Girl" photograph).
- Content depicting child nudity in the context of religious rituals or ceremonies (for example, baptisms).
- Newsworthy content that depicts child nudity in the context of famine, genocide, war crimes, or crimes against humanity.

The scanning of Cloud content as it appears in Adobe's legal documents and publicly available documentation is part of Section 8.2. This section also includes a description of the CSAM detection methods as well as the review and reporting process.

[93] Adobe, Adobe Transparency Center, Policies: Harmful Content: Child Safety, URL: https://www.adobe.com/trust/transparency/content-policies/harmful-content/child-safety.html, last viewed 14 November 2024.

[94] Adobe, Adobe Transparency Center, Harmful Content, URL: https://www.adobe.com/trust/transparency/content-policies/harmful-content.html, last viewed 24 December 2024.

2 Personal data and data subjects

When examining the privacy risks of a data processing operation, it is important to consider what types of data of which groups of data subjects are being processed.

This section lists all types of data from different groups of data subjects. Section 2.1 starts with a summary of Adobe's information about the personal data it processes in relation to the use of Adobe. Section 2.2 provides an overview of potential processed categories of personal data and lists the data subjects that may be involved when using the Adobe Creative Cloud and Adobe Document Cloud. Section 2.3 contains the results of the analysis of the network generated through the tests as described in the technical appendix. This section concludes with a subsection on the DSARs.

2.1 Personal data processed by Adobe

2.1.1 Types of personal data processed by Adobe

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

Table 4: Types of personal data processed by Adobe

#	Type	Description
1	Identifiers and contact information	Name, email address, telephone number, postal or physical address, country
2	Commercial and transaction information	Payment/billing information, licenses purchased, eligibility information, content of and information provided through customer support and other communications, types of Services and Software of interest.
3	Professional or other demographic information	Date of birth, company, title, occupation, job function, expertise, company details such as the size, industry and other information about the company the user works.
4	Analytics and other electronic network activity	IP address, browser, mobile device ID, browser extensions connected to the user's Adobe accounts, cookies.
5	Adobe Software activation and automatic updates	Analytics or other electronic network activity information, such as details of the user's device, it's manufacturer, model and IP address, the Adobe Software used including version, date of activation, successful and unsuccessful updates, the user's product serial number.

6	Adobe emails	Emails Adobe sends may include a technology (web beacon) that collects Analytics or other electronic network activity, such as whether the user received or opened the email or clicked in a link in the email (this can be opted out)
7	Adobe online advertising	Analytics or other electronic network activity such as which ads are displayed, which ads are clicked on and where the ad was displayed.[95]
8	Buttons, tools, and content from other companies	Information about user interactions with features like Facebook "Like" buttons, information from the user's browser when interacting with embedded content. Device and application data collected by Google reCAPTCHA.
9	Adobe's social networking pages and social sign-on services	Account information and public profile data and engagement insights.
10	Adobe "acting on your behalf"	In certain instances, Adobe is acting only on your behalf for personal information collected and processed by our services (for example, for the address book contacts shared by users when entering recipient information).
11	"Content to deliver features requested by you"	"Adobe offers certain features that let you edit and organize your photographs, videos, and other types of content using characteristics like face and voice (e.g., you can group similar faces, places, and image characteristics within your collection), and such characteristics may be considered biometric identifiers or biometric information under certain US laws or other applicable privacy laws."
12	Visiting physical offices	N/A
13	Services and Software information	Analytics or other electronic network activity, (IP address, browser and device details, referring webpage and search terms leading to Adobe websites, usage and navigation data from Adobe Services and Software, analysis of content usage (subject to user consent). Demographic and profile information. *"Commercial and transaction information such as content that includes personal data which is sent or received using an online feature of Adobe Services and Software, or which is stored on Adobe servers, such as documents, photos, videos, activity logs, direct feedback*

[95] See for AdChoices / additional opt-out choices Section 3.2.1.2.

		from you, metadata about your content, user generated requests such as search terms, prompts such as text, images, videos, audio, etc., inquiries, feedback, and other information you may disclose when you access or use our Services and Software as well as any information the Services and Software returns in response to such requests."
14	Customer Data	See Section 2.1.2.1 for the definition

As stated in row 6 of the table above, some emails sent by Adobe may contain web beacons. Individuals can make choices about what emails they want to receive in a number of ways. They can make choices in the user preference centre through their Adobe account (https://account.adobe.com/communication). In addition to this, users can opt out by clicking an unsubscribe link in the footer of an email from Adobe, send an email to DPO@adobe.com, call customer service to request to opt-out from certain types of email communication, or submit a request via the privacy contact form on Adobe.com.[96] See also Section 3.2.2.

2.1.1.1 Profile Information and Usage and Technical information

Adobe arranged the personal data returned in the DSAR into two broad categories: Profile Information (e.g. personal data in which the data subject is directly identifiable) and Usage and Technical information (in which Adobe identified data associated with the specific user ID). The following paragraphs list the data included in these broad categories. In the third column of the tables, the number refers to the types of personal data listed in Table 4.

Table 5: Profile information

Category	Description	#
Profile data	This sets out the basic information for your user profile (name, type of account, email)	1
Service Account details	This sets out the services (including those that have been cancelled or terminated) that are specifically associated with your Adobe ID	5 13
Case notes and email activity	These are details of messages (email and SMS) we have associated with your account.	1 2 5 6 10 13

[96] Email Adobe 13 December 2024.

Marketing Database information	This sets out the permissions and profile information related to marketing.	1 2 3 6 7 13
Creative Cloud Engagement Services	This contains information about the specific configurations of your products and if you have used any resources (such as how to guides).	1 13
Fonts Data	This contains information about your use of Adobe fonts, capturing certain types of activity (e.g., font used).	1 13
Sign Data	This contains data associated with Adobe Sign and your user Profile. It includes security verification data, dates of modification, some limited account activity and settings that are in place.	1 5 13
Portfolio Data	This contains data related to the Adobe Portfolio products assigned to your Adobe ID that users can have access to (e.g., Portfolio, Behance, Lightroom).	1 13

Table 6: Usage and Technical Information

Category	Description	#
Product and Services Data	This is operational, cloud and user behavioural data for Adobe's Creative Cloud and Document Cloud, web, mobile and desktop apps and services. It is best understood as product usage data, showing how a particular user navigates and deploys Adobe products (e.g., individual Generative AI prompts).	13
Integrity Data	Integrity data comes from a service incorporated into the code of Adobe desktop applications that serves to capture certain information about the software license and the device on which it is installed in order to help prevent the pirating of genuine Adobe software.	5 13
Adobe Identity Data	This is operational data about Adobe account activity, such as logins, changes made to user account information, when an account is added to an organization, and when an organization makes changes to its users' accounts.	13

All of the three categories above would fall under the category of 'Services and Software information' as described in Table 4. Integrity data comprises of both 'Services and Software information' data, as well as 'Adobe Software activation and automatic updates'.

2.1.1.2 Special category data

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*"

Adobe can process several types of special category data through user generated content. In addition to this Adobe Express includes features that process biometric data.

- Automatically adding captions to a video (voice recognition)[97]
- Making an animated character talk with your own voice[98]

In this DPIA the focus will be on the biometric data Adobe processes when using Adobe Express and the question if Adobe can use these biometric data for the purpose of uniquely identifying a natural person.

Article 4 (14) of the GDPR contains the following definition of biometric data:

> *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."*

There are three cumulative criteria for personal data to constitute biometric data as defined in the GDPR:

1. **The nature of the data**: it must be data to the physical, physiological or behavioural characteristics of natural persons.
2. **The means and manner of processing**: it must concern personal data 'which are the result of specific technical processing'.
3. **The purpose of processing**: unambiguous identification of that natural person is possible or is confirmed.

Adobe asserts that the processing of voice recordings does not constitute the processing of special category data:

> *'Adobe Express users can automatically add captions to a video using the Caption Video feature. Users can also use Animate characters to create an avatar using their own voice or an audio file. However, Adobe does not use audio from Caption Video or Animate characters for the purposes of identifying individuals based on their biometric data nor does Adobe otherwise process the voice data for any other purpose other than that*

[97] Adobe, 'Caption videos', Last updated on Oct 21, 2024, URL: https://helpx.adobe.com/express/create-and-edit-videos/edit-videos/caption-video.html.

[98] Adobe, 'Animate Characters, Last updated on Jan 24, 2025, URL: https://helpx.adobe.com/express/create-and-edit-videos/edit-videos/animate-from-audio.html.

which the user has requested. The voice recording features of Adobe Express does not meet the cumulative criteria to constitute biometric data.'[99]

However, Adobe's Privacy Policy states that Adobe may process data classified as biometric identifiers or biometric information under applicable privacy laws through certain features. The privacy policy also clarifies that the features involving such data are disabled by default, and it is up to the user to activate them, indicating that Adobe likely relies on consent as the legal basis for this type of processing.[100]

In any case, if special category data is processed by Adobe through the use of Creative Cloud or Document Cloud, Adobe does so in the capacity of a data processor on behalf of the Customer except in situations in which it processes content data for its own purposes.

2.1.2 Personal data in the legal documentation

2.1.2.1 Adobe's DPA (June 2024)

The DPA template does not provide a comprehensive or definitive list of personal data. Exhibit 1 to Adobe's DPA[101] describes the subject matter and details of the processing of personal data.[102] It states that the types of personal data are determined and controlled by 'Customer' in its sole discretion, *"and may include, but are not limited to:*

(a) Identification and contact data (e.g. name, date of birth, email address, telephone number, title, address),
(b) Transaction information related to how individuals use Customer's services or
(c) IT information, (e.g. IP addresses, cookie data, location data).[103]*"*

'Personal Data' in Adobe's DPA (June 2024) means 'Customer Data' that relates to an identified or identifiable natural person or as otherwise defined under applicable Data Protection Laws.[104] 'Customer Data' has the meaning set forth in the Agreement.[105]

According to the Enterprise General Terms (which are part of the Agreement) 'Customer Data' means any (1) information or (2) material, such as audio, video, text, or images, that are imported into the Cloud Services by or on behalf of Customer from Customer's internal data stores, third-party data providers, or is collected via the Distributed code, and is used in connection with Customer's use of the Products and Services. Customer Data includes "Customer Content" if referenced in the Agreement.[106] The Enterprise General Terms adds to

[99] Email Adobe to SURF, 21 March 2025.

[100] Adobe Privacy Policy, 'How we process your content to deliver features requested by you', Last updated: June 18, 2024, URL: https://www.adobe.com/privacy/policy.html.

[101] Adobe DPA dated June 2024.

[102] Article 3.3 DPA, Adobe DPA Cloud Services Only), June 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/DPA-WW.pdf.

[103] Exhibit 1 to Data Processing Addendum - Details of Data Processing, Adobe DPA Cloud Services Only), June 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/DPA-WW.pdf.

[104] Article 1.11 Adobe DPA (June 2024).

[105] Article 1.4 DPA Adobe DPA (June 2024).

[106] Article 1.11 Adobe General Terms (2024v1), (2024v1), Effective Date: 8 March 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf. "Customer Content" is not

that Adobe may develop, modify, improve, support, customize, and operate its products and services based on information that Adobe collects on Users' interactions with the Products and Services (Usage Information). Such Usage Information does not include any Customer Data.

2.1.2.2 Content Data

According to its Privacy Policy[107], Adobe analyses the user's content and its characteristics using automated techniques to enable the operational use of the system. This includes both content stored locally on the user's device as well as content that is uploaded to Adobe's services ("cloud content"). [108] Users with a business account are automatically opted out of content analysis for product improvement.[109] Adobe reserves to right to perform analytics on cloud content data (not local data) of non-business users (subject to their opt-out rights), in order to improve the service, provide recommendations, and 'customize the experience'. *"Insights from Content Analytics may be used to inform a marketing to you, subject to your opt-out rights regarding our marketing".* [110]

Adobe analyses the user's content and its characteristics using automated techniques or with human review, in case of illegal and abusive cloud content, and public and shared cloud content. *"Cloud Content may be automatically scanned to ensure we are not hosting illegal or abusive content, like Child Sexual Abuse Material. Human review may occur when your Cloud Content is flagged or reported as illegal or abusive".* All public and shared Cloud Content is subject to review for intellectual property issues and safety issues (for example, violence and nudity). This also applies to business and education organisations.[111]

When users share their cloud content with others using Adobe's software and services (Creative Cloud products, as well as cloud storage related to Acrobat), Adobe reserves the right to automatically review this shared cloud content to flag abusive behaviour (such as spam or phishing). Additional human review may occur when the user makes their cloud content publicly available.[112] Adobe's scanning of Content for Child Safety is described in Section 1.6.

---

referenced as SURF negotiated to enter the updated Terms and Conditions. This referenced part of the Customer Data definition was included to cover scenarios whereby certain customers are still on some older versions of terms that do reference the concept of "Customer Content". However, this is not relevant to SURF - SURF negotiated and entered the 2024 version that does not have the concept of Customer Content anymore as these have been consolidated into one single definition. (Email Adobe 28 March 2025).

[107] Adobe Privacy Policy, 'How does Adobe use the information it collects about you, and what are the legal bases for these uses?', Last updated: 18 June 2024, URL: https://www.adobe.com/privacy/policy.html.

[108] Adobe Privacy Policy, 'How does Adobe use the information it collects about you, and what are the legal bases for these uses?', Last updated: 18 June 2024, URL: https://www.adobe.com/privacy/policy.html.

[109] Adobe, Content analysis FAQ, last updated 30 July 2024, "Also applies to Adobe Creative Cloud, Document Cloud ", URL: https://helpx.adobe.com/manage-account/using/machine-learning-faq.html, last viewed 16 November 2024.

[110] Adobe Privacy Policy, 'How does Adobe use the information it collects about you, and what are the legal bases for these uses?', Last updated: 18 June 2024, URL: https://www.adobe.com/privacy/policy.html.

[111] Email Adobe 13 December 2025.

[112] Adobe Privacy Policy, 'How does Adobe use the information it collects about you, and what are the legal bases for these uses?', Last updated: 18 June 2024, URL: https://www.adobe.com/privacy/policy.html.

2.1.2.3 Student Data Terms

As per Adobe's Student Data Terms, 'Student Data' means (1) '*Student Personal Information'* and (2) *'Student Assets'.*[113]

'Student Personal Information' is: *"information provided to the Services by a School, User, parent or legal guardian, or gathered by Adobe during use of the Services pursuant to these Terms, that can be used to identify or contact a particular Student or that, alone or in combination, is linked or linkable to a specific Student so as to allow a reasonable person in the School community, who does not have knowledge of the relevant circumstances, to identify the Student with reasonable certainty or that would otherwise be regarded as personally identifying information relating to a Student under applicable laws."*[114]

'Student Assets' are *"the files, data, and content generated or created by Students through their use of the Services pursuant to these Terms, excluding any underlying Adobe Software and/or Services."*[115]

2.2 Possible types of data subjects

Data subjects are all identified or identifiable natural persons within data processing operations. In other words, the individuals about whom personal data are processed.

Adobe lists as possible groups of data subjects: Customer's prospects, customers, business partners, vendors, and employees.[116]

The end users of Adobe Creative Cloud for Education are employees, contractors, students and (temporary) workers of the educational institutions.

Given the complexity of Adobe Creative Cloud, this DPIA assumes users will be at least of secondary school age (thus excluding primary school students). As a result, some data subjects may still be under the age of digital consent. If consent is the legal ground for the data processing, verified parental consent will be necessary when the data subject has not yet reached the age of digital consent. The age of digital consent in The Netherlands is 16 years (Article 6(1)a in conjunction with Article 8(1) GDPR and Article 5(1) of the UAVG). This will be assessed in Part B of this DPIA. In the Student Data Terms, students above the legal age of consent are categorized as "adult students".

As described in Section 1.1 Adobe offers different plans for K-12 (primary and secondary) schools, and for Higher Education Institutions (HED). Adobe ensures a higher level of (data)protection for K-12 students, provided the correct ID has been assigned (Enterprise or Federated).

[113] Article 1.7 Student Data Terms. "Student Data does not include any information received by Adobe outside the context of the provision of the Services pursuant to the Terms."

[114] Article 1.8 Student Data Terms.

[115] Article 1.6 Student Data Terms.

[116] Point 7 of the Exhibit 1 to Data Processing Addendum - Details of Data Processing, Adobe DPA dated June 2024.

2.3 Outgoing Traffic Analysis

Section 2 of the Technical Appendix describes in detail the tests performed by Privacy Company while collecting outgoing and incoming traffic to Adobe services. Tests were performed between 11 September 2024 and 25 September 2024. On a high level, the following tests were conducted:

- Navigating to the cookie banner (web).
- Visiting the admin console and adding users and an admin.
- Downloading and installing Creative Cloud on the desktop (Windows and Mac).
- Generating videos, posters, thumbnails and an AI alter ego, and bullying a classmate in Adobe Express (web).
- Merging PDFs, exporting PDFs and signing feedback in Adobe Acrobat (Windows, Mac and web).
- Several actions in Adobe Photoshop (Windows, Mac and web).
- Image generation in Firefly (web).

The sections below outline the observed traffic: first party traffic (directly to Adobe) in Section 2.3.1 and traffic to third parties in Section 2.3.2. For every endpoint, the party involved, and personal data exchanged, are briefly discussed. Full details can be found in the Technical Appendix.

2.3.1 First-party traffic

During testing, Privacy Company observed several Adobe first party domains receiving data. Such traffic is to be expected, especially for the web applications. Some highlights of the first-party traffic are discussed below. Full details of this traffic can be found in Section 3.1.1.1 of the Technical Appendix.

2.3.1.1 Adobe telemetry endpoints

Across the majority of the tests performed, Adobe was observed to send telemetry data to first-party domains. These endpoints receive:

- several unique identifiers and data about actions taken by users while using Adobe services;
- the name of the device of the user, which may include personal information (for example “MacBook Pro Van [Data Subject’s Name]”), in case of desktop applications;
- cookies whose storage period and values qualifies them to be tracking cookies.

Exact data collected varies per application and access method, e.g., web-based applications generally send cookies when collecting telemetry, whereas desktop-based applications may send device identifiers not available to web applications.

Data for (some) of the telemetry events was returned in the DSAR response, but not all observed telemetry events were returned in the response. See Section 2.4.3.4 for details.

Adobe informed SURF in a statement that some telemetry is essential for the operation of a product and cannot be disabled. Adobe also states that that the storage period for (mandatory and optional) telemetry data is four years.[117]

For users with business profiles, only essential telemetry should be collected. Personal accounts can opt-out of telemetry.[118] Privacy Company conducted tests with enterprise licenses and thus using business profiles, so observed telemetry was either deemed essential by Adobe or sent by mistake.

Some of the telemetry observed in the traffic seems to display users navigating through the applications (on a high level).

For more information on telemetry, see Section 3.1.1.1.1 of the Technical Appendix.

2.3.1.2 Adobe Firefly

As described in Sections 3.1.1.1.3 and 3.1.1.1.8 of the Technical Appendix, Privacy Company has observed data being sent to multiple domains associated with Adobe Firefly services. These data include, amongst other things, the text of prompts, images, unique identifiers, random seeds, and credentials sent to Amazon Web Services to request the retrieval of the generated images. This data is to be expected, as Adobe Firefly is an 'on-demand' service backed by online infrastructure.

With generative AI services such as Firefly, it is necessary to have insight into the backend processing to assess risks. Because of this, understanding what is done with the data sent to these domains is outside the capability of Privacy Company's test environment. Privacy Company describes the techniques and methods used by Firefly services in Section 8.1, including a description of the random seeds. This is based upon publicly available documentation from Adobe.

An example of the traffic sent to Adobe Firefly services when a generated image is requested can be found in Section 3.1.1.2.1 of the Technical Appendix.

2.3.1.3 Adobe Experience Cloud

During testing of several web-based Adobe services (such as Photoshop), Privacy Company observed traffic to "adobe.tt.omtrdc.net", containing several unique identifiers. According to Adobe's documentation[119], "omtrdc.net" is a tracking server for Adobe Experience Cloud analytics services. Adobe clarified that this traffic was used to personalise the website.[120]

---

[117] Email Adobe to SURF, 28 March 2025.

[118] Adobe, Usage Data FAQ: Creative Cloud and Document Cloud Apps, URL: https://www.adobe.com/privacy/app-usage-info-faq.html, last updated 18 June 2024.

[119] Adobe Experience League, "How to identify your analytics tracking server and report suite ID", URL: https://experienceleague.adobe.com/en/docs/analytics-learn/tutorials/implementation/implementation-basics/how-to-identify-your-analytics-tracking-server-and-report-suites, Last updated 11 October 2023.
Adobe Experience League, "Use an Analytics tracking server", URL: https://experienceleague.adobe.com/en/docs/target/using/integrate/a4t/analytics-tracking-server, Last updated 24 April 2023.

[120] Email Adobe to SURF, 28 March 2025.

A further description of the data sent to Adobe Experience Cloud analytics services can be found in Section 3.1.1.1.9 of the Technical Appendix.

2.3.1.4 Behance

Behance is an Adobe social media platform designed for individuals to share creative works.[121] Behance is not available for K-12 users. During testing, several domains associated with Behance were observed receiving data.

Section 3.1.1.1.10 of the Technical Appendix summarises these cookies and provides additional information. None of these cookies were documented in the Adobe cookie banner (see Section 3.2.1).

More information about data shared with Behance can be found in Section 3.1.1.1.10 of the Technical Appendix. See the textbox at the end of Section 2.3 'Update after completion part A' which provides clarification about the purpose of the cookies and mentions the fix that was made to the cookie consent banner.

2.3.1.5 Other first-party Adobe services

Privacy Company observed various cookies and unique identifiers being sent to Adobe authorisation and licensing services as would be expected for online services (Sections 3.1.1.1.4 and 3.1.1.1.5 of the Technical Appendix). Privacy Company also observed unique identifiers sent to Adobe.io domains (Section 3.1.1.1.11 of the Technical Appendix) and Adobe Sensei services (Section 3.1.1.1.8 of the Technical Appendix) that seem to provide core online services.

Cookies containing unique identifiers were also observed sent to be sent to domains of the Adobe Help Center (Section 3.1.1.1.6 of the Technical Appendix) and various domains associated with Adobe Acrobat services (Section 3.1.1.1.7 of the Technical Appendix).

Many of the same cookies are used by the domains described above. A summary of these cookies is included in Section 2.3.3.

2.3.1.6 Demdex

Demdex is a part of Adobe's Audience Manager and Adobe Experience Platform Identity Service.[122] Privacy Company observed several domains associated with Demdex services. This traffic includes tracking cookies and other unique identifiers.

Privacy Company observed that the cookie banner used on these web-based apps worked inconsistently. For example, on "stock.adobe.com" additional data was shared to first and third parties by Demdex services regardless of the choice made on the cookie banner. This included a myriad of third-party advertising cookies.

More information about Demdex cookies and associated tracking technologies can be found in Section 3.1.1.1.2 and 3.1.2.12 of the Technical Appendix. See the textbox at the end of Section

[121] Adobe, "Guide: Intro to Behance", URL: https://help.behance.net/hc/en-us/articles/204483894-Guide-Intro-to-Behance, Last Updated "3 Years Ago", last viewed 21 January 2024.

[122] Adobe Experience League, "Understanding Calls to the Demdex Domain", URL: https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/demdex-calls, Last updated 19 August 2021.

2.3 'Update after completion part A' which provides clarification about the Demdex cookies and mentions the fix that was made to the cookie consent banner.

2.3.2 Third-party traffic

During testing, Privacy Company observed data being sent to various third parties. A full list of these third parties can be found in Section 3.1.2 of the Technical Appendix. Below Privacy Company provides a summary of a few of these third parties.

2.3.2.1 CDN Providers

Privacy Company observed during testing web traffic sent to multiple CDN (content delivery network) providers that host content for Adobe. In all cases, the responses of these CDN-providers included headers or cookies that were set by the CDN-provider (based on the name of the header and/or cookie). This means that the encrypted (HTTPS) connections from Adobe are terminated at the CDN-provider and a new encrypted connection is established to the end-user. Hence, the transmitted data is handled unencrypted by the CDN-providers and is modified by the CDN-providers. This is a common scenario but does mean that any personal data transmitted through the CDN-provider is processed by the CDN-provider (either as an independent or joint controller, or as a processor).

Adobe provided in a statement to SURF a description of Adobe's relationship with the CDN Providers described in this section:

> *"…all personal data transmitted through the CDN-provider is processed by the CDN-provider as a data processor for Adobe's purposes only."*[123]

2.3.2.1.1 Akamai

Across multiple tests, Privacy Company observed traffic to domains hosted by Akamai, a cloud computing provider[124]. This includes www.adobe.com, including authentication cookies set on that domain.

Adobe explained:

> *"Akamai provides Adobe with a content delivery network to help provide a geographically distributed high availability network and assist performance by distributing the service spatially relative to end users. Fundamentally Akamai's processing of Adobe customer is significantly limited to nominal processing. As per our Data Processing Agreement with Akamai, they only process limited personal data (e.g., login credentials and IP address data). Akamai also assists with providing tag management software as part of the Adobe Experience Platform Tags product (formerly known as Launch). This is used for installing many of the digital experience solutions. It helps provide users the option of hosting installation libraries for web and mobile devices on the Akamai content delivery network.*
>
> *Detailed Adobe customer user personal data does not pass through Akamai. Akamai simply hosts a library across their global edge nodes to facilitate faster access and download. As part of this process, IP addresses and limited login credential data are required for internet communications so Akamai server logs may contain the IP address*

[123] Email Adobe to SURF, 28 March 2025.

[124] Akamai, "Power and Protect Business Online", URL: https://www.akamai.com/, Last viewed 23 January 2025.

of incoming requests (like any other servers/content delivery networks on the internet), but there would be no other identifying data tied to it (as Adobe does not route any hit data or user information through Akamai).

In terms of specific products, we can confirm that Stock and Photoshop don't use Akamai directly but as above it can be used to host installation libraries. Similarly, Express does not make any direct calls to Akamai domains, but some static data associated with an installation may be stored purely to enhance delivery speed (but this wouldn't contain detailed personal data). This engagement is reflected in our Data Processing Agreement with Akamai."[125]

This explanation seems to focus on the content delivery functions of Akamai but misses the point that Adobe's main domain "http://www.adobe.com" is fully proxied by Akamai and any identifying cookies set on that domain will be processed by Akamai.

Further description of the observed traffic to Akamai domains can be found in Section 3.1.2.5 of the Technical Appendix.

2.3.2.1.2 Fastly

Privacy Company observed traffic to the domain "jil.adobe.com". This domain is proxied through Fastly, a CDN-provider[126]. Privacy Company observed that, when using Adobe services, user details are sent using this domain to provide the user profile of the user (i.e. Fastly services are used to request a user id and return name/email/type value for the user).

2.3.2.1.3 Cloudflare

Privacy Company observed traffic to Cloudflare[127] servers during the installation of applications. Privacy Company observed the data being sent to the endpoint "auth.services.adobe.com", which is a Cloudflare endpoint. Observed data sent includes cookies and user email addresses (for Adobe IDs this data would also include user passwords).

2.3.2.1.4 Amazon Web Services

Privacy Company observed traffic to Amazon Web Services during testing. In Section 8.1.1 of this DPIA and Section 3.1.1.1.3.1 of the Technical Appendix, Privacy Company discusses the use of Amazon Web Services during the use of Firefly tools to generate images[128]. The tests during which this traffic was observed are discussed in Section 3.1.2.2 of the Technical Appendix. Additional discussion of the role of Amazon Web Services in Adobe Cloud services can be found in Section 5.3.1.1.

2.3.2.2 Branch.io

Privacy Company observed traffic to the company 'Branch'[129], a company which offers tools for online marketing, receiving tracking cookies and unique IDs based on browser fingerprinting. More information about Branch.io, including an example of the tracking cookie, can be found in Section 3.1.2.1 of the Technical Appendix.

[125] Email Adobe 24 January 2025.

[126] Fastly, "A more powerful global network", URL: https://www.fastly.com/, Last viewed 23 January 2025.

[127] Cloudflare, "Connect, protect, and build everywhere", URL: https://www.cloudflare.com/, Last viewed 4 February 2025.

[128] Amazon, "Cloud Computing with AWS", URL: https://aws.amazon.com/what-is-aws/, Last viewed 4 February 2025.

[129] Branch, "All channels lead to you", URL https://www.branch.io/, Last viewed 20 November 2024.

2.3.2.3 Sentry.io

Sentry.io[130] is a company that provides application monitoring software. Privacy Company observed unique identifiers and telemetry being sent to this endpoint during testing. More information about Sentry.io can be found in Section 3.1.2.4 of the Technical Appendix.

2.3.2.4 New Relic

New Relic[131] is a company that offers web monitoring and other tracking services. Privacy Company observed traffic during testing being sent to domains owned by New Relic across all test scenarios. The data sent to these endpoints includes information about the actions a user has taken on a specific page.

Adobe explained:

> *"New Relic, Inc. is an Adobe service provider and sub-processor. Adobe uses New Relic's technology solutions to monitor operational performance of certain Adobe products and provide alerts as to telemetry data to help Adobe identify critical issues. Examples of operational performance monitoring metrics include data about load times or error rates. New Relic doesn't process or transform the data after collection other than nrql queries/ dashboards to view and alert on patterns. This is mostly metrics and alerting data (used to monitor operational performance).*
>
> *To do this New Relic processes minimal personal data of customers (e.g., IP addresses in CDN logs are used in New Relic to detect BOT traffic and bad actors in order to update firewall rules and maintain site performance). Adobe has worked with New Relic for over a decade, with regular annual recertifications and a data processing agreement."*[132]

More information about New Relic can be found in Section 3.1.2.6 of the Technical Appendix.

2.3.2.5 Fingerprint

Fingerprint is a company that assigns unique identifiers to visitors of a website. Privacy Company observed traffic to Fingerprint domains during testing. Fingerprint advertises that its services can be used to track users across multiple first party domains.[133] Privacy Company was unable to read the content of the data sent to Fingerprint domains during testing. More information about Fingerprint can be found in Section 3.1.2.10 of the Technical Appendix.

2.3.2.6 UserVoice

Adobe has partnered with third party "UserVoice"[134] to allow users to provide feedback on services. Privacy Company has identified several cookies being sent to this domain during the use of several Adobe web-based services. While none of these cookies have a storage period that qualifies as a tracking cookie, several of the cookies containing unique identifiers were not documented in Adobe's cookie banner. More information about UserVoice can be found in Section 3.1.1.1.10 of the Technical Appendix.

---

[130] Sentry, "Code breaks, fix it fasters", URL: https://sentry.io/welcome, Last viewed 20 November 2024.

[131] New Relic, "Intelligent Observability", URL: https://newrelic.com/, Last viewed 20 November 2024.

[132] Email Adobe 24 January 2025.

[133] Fingerprint, "Identify Every Visitor", URL: https://fingerprint.com/, Last viewed 26 November 2024.

[134] Adobe, "How to use UserVoice to request new features and report bugs", UR:" https://helpx.adobe.com/x-productkb/global/how-to-user-voice.html, Last updated 12 July 2024.

2.3.2.7 Google DoubleClick

Privacy Company observed traffic to Google's DoubleClick[135] services during the testing of Adobe Express's web-based services on new.express.adobe.com. The test user had not opted in to sharing data with Google. More information about Google DoubleClick can be found in Section 3.1.2.7.1 of the Technical Appendix.

2.3.2.8 Third-party hosting services

Privacy Company observed that Adobe uses several third-party services to host content on Creative Cloud services. This includes Simplecast (Section 3.1.2.8 of the Technical Appendix), Spotify (Section 3.1.2.13 of the Technical Appendix), YouTube (Section 3.1.2.7.2 of the Technical Appendix), and Vimeo (Section 3.1.2.9 of the Technical Appendix).

2.3.2.9 Other third-party domains

Privacy Company has observed traffic to several other third parties that provide services to Adobe.

Among these third parties, the following were observed receiving unique identifiers beyond user IP addresses:

- Forter, a company that offers multiple services including fraud prevention[136] (Section 3.1.2.3 of the Technical Appendix).
- Arkoselabs, a company that offers fraud prevention and other services for online platforms. In a case study of Arkoselab's work with Adobe, Arkoselabs states that Adobe has used Arkoselabs services to "to enhance detection techniques around potential fraudulent accounts"[137].

2.3.3 Observed Cookies

As described in Section 3 of the Technical Appendix, Privacy Company has analysed the cookies observed in the network traffic generated by the use of Adobe Creative Cloud and Document Cloud. A summary of cookies per observed domain can be found in Section 3.1.1.1 and 3.1.2 of the Technical Appendix.

Privacy Company considers cookies with a storage period longer than a single browsing session and containing unique identifiers as (possible) tracking cookies. Privacy Company observed tracking cookies being used by both Adobe domains and third-party domains.

Not all cookies observed during testing were included in Adobe's cookie banner. This takes two forms:

1. cookies whose names are not in the cookie banner at all (type 1).
2. cookies whose names are in the cookie banner, but whose observed hostnames are different than those reported in the cookie banner (type 2).

[135] Google, "DoubleClick Digital Marketing", URL: https://support.google.com/faqs/answer/2727482?hl=en, Last viewed 20 November 2024.

[136] Forter, Identity Intelligence for Digital Commerce, URL: https://www.forter.com/, Last viewed 20 November 2024.

[137] Arkose Labs, "Adobe Reduces Fabe Account Risk and Improves User Experience with Arkose Labs", URL: https://www.arkoselabs.com/resource/adobe-reduces-fake-account-risk-and-improves-user-experience-with-arkose-labs-case-study/, Last 22 January 2025.

This amounts to the same issue – Adobe's cookie banner (as documented by Privacy Company on 3 December 2024) was incomplete.

A summary of these cookies is in Section 3.1.3 of the Technical Appendix. Several of these cookies meet the criteria of being tracking cookies.

In response to the draft of Part A of the DPIA, Adobe indicated to be investigating the root cause of the missing or misclassified cookies, *"in particular whether it was a faulty scan or operator error, and will incorporate any relevant learnings into our cookie identification and classification process going forward."*[138]

Update after completion of Part A

Privacy Company identified several issues during testing, which can be categorised as:

- Incomplete information in the cookie banner
- The cookie banner not functioning as expected
- Traffic exchanged for analytics, product improvement and personalisation with unclear purposes

In response to this, Adobe promptly and diligently improved their products to resolve these issues. On several occasions, Privacy Company observed new issues, which Adobe also promptly addressed.

Incomplete cookie banner

Adobe provided a statement to SURF that "Missing cookies will be added to the banner" for all missing cookies (e.g., Behance, UserVoice).[139] Privacy Company performed spot checks in November 2025, and the missing cookies were now listed in the cookie banner.

Furthermore, Adobe provided the following as an explanation for the purposes of the Behance cookies:[140]

> *'…during sign in for all users, including those designated as K12 students, cookies are set in the Behance domain as part of the service in order to allow users with access to Behance to seamlessly connect once they are logged in.'*

Non-functional cookie banner

On 31 January 2025, Privacy Company received an additional response from Adobe relating to the cookie banner on stock.adobe.com. Adobe stated that the banner has been fixed, and this was confirmed by Privacy Company in additional testing on 5 February 2025.

On 7 May 2025, after communication with Adobe, Privacy Company observed that Google DoubleClick no longer receives data from users on new.express.adobe.com when the user opts out of additional sharing in the cookie banner.

[138] Email Adobe to SURF, 28 March 2025.

[139] Email Adobe to SURF, 28 March 2025.

[140] Email Adobe to SURF, 28 March 2025.

In August 2025, Privacy Company informed Adobe that several Demdex, DPM and Everesttech tracking cookies were being set without consent. Adobe resolved these issues promptly or retired the site that set these cookies.[141]

Furthermore, Adobe implemented a technical solution in April 2025 that makes it impossible to users of educational institutions in the Netherlands to opt-in to advertising cookies. If the user chooses to opt-in before logging in, they will be automatically opted out as soon as they login and are identified as an educational user.[142]

Analytics, product improvement and personalisation
During testing, Privacy Company regularly encountered cookies to Demdex or Adobe Target (omtrdc.net).

Adobe clarified that Demdex is used as part of Adobe Audience Manager, and asserted any cookies are only used for *'visitor identification'*:[143]

> *"For clarity, Demdex was a company providing audience management solutions, but it was acquired by Adobe and rebranded as Audience Manager. Demdex, including the demdex.net domain is owned by Adobe. However, when Adobe sets the Demdex cookie on Adobe sites it is technically set in the demdex.net domain rather than the adobe.com domain which makes it look like a third party cookie. Practically speaking, however, because, as you note, Adobe owns Demdex, the data collection using Demdex on Adobe sites functions like a first party cookie."*

Adobe also clarified:[144]

> *"Adobe Target is used to personalize tutorial content within the Photoshop Discover tab so that the most relevant tutorial information is made available to a particular user."*

Adobe made changes so that Adobe Target is no longer used if a user opts out of all cookies.[145] This was verified by Privacy Company in November 2025. During these spot checks, traffic to Demdex or Adobe Target was no longer observed.

These updates have been taken into account in parts B-D of this DPIA.

2.4 Data Subject Access Requests

This section is divided into four subsections: Section 2.4.1 addresses how access rights are integrated in the various legal documents. Section 2.4.2 discusses the submitted DSARs and the timeline. Adobe's response is detailed in Section 2.4.3 and further discussed in Section 2.4.4.

[141] Email Adobe to SURF, 31 October 2025.

[142] Email Adobe to SURF, 31 October 2025.

[143] Email Adobe to SURF, 28 March 2025.

[144] Email Adobe to SURF, 31 October 2025.

[145] Email Adobe to SURF, 31 October 2025.

2.4.1 Incorporation of Access Rights in legal documentation

Access Rights are incorporated in the various legal documents.

Adobe's DPA includes a clause that Adobe will promptly inform the Customer / Participant (school) of any Data Subject Access Request (DSAR) in connection with the Adobe Cloud Services licensed by the school and imposes the responsibility of handling such requests in accordance with European Data Protection Laws with the school.

The Student Data Terms include a clause that requires schools to establish reasonable procedures by which parents, legal guardians, or "eligible students" may request access to Student Data generated through the services.[146]

See a comparison of the clauses in the table below.

Table 7: Comparison provisions on Access Rights

Adobe DPA (June 2024) (Article 9.1)	Student Data Terms (Article 9.1)
"Individual Rights. Adobe will promptly notify Customer if Adobe receives a request from a Data Subject relating to Customer's use of the Cloud Services, including where the Data Subject seeks to exercise any of its rights under applicable Data Protection Laws (collectively, "Data Subject Request"). The Cloud Services provide Customer with controls that Customer may use to assist it in responding to Data Subject Requests. Customer will be responsible for responding to any such Data Subject Requests. To the extent Customer is unable to access the relevant Personal Data within the Cloud Services, upon Customer's written request, Adobe will provide commercially reasonable cooperation to assist Customer in responding to a Data Subject Request."	*9.1. Parent Access Requests. Customer will establish reasonable procedures by which a parent, legal guardian, or eligible Student may request access, correction, or deletion of Student Data generated through the Services. Upon request by the Customer, Adobe will work with Customer and its School(s) as needed to facilitate such access."*

2.4.2 DSAR request

To assess the ability for data subjects to perform their rights and to get more insight in the personal data that is processed by Adobe, Data Subject Access Requests (DSAR) were submitted to Adobe by two data subjects.

The DSARs requested all personal data, but especially:

1. Technical logs about the usage of Adobe Creative Services
2. Security logs
3. Cookie data collected while using the Adobe Creative Services and applications

[146] Article 9.1 Student Data Terms.

4. Telemetry and/or diagnostic data

The DSARs were submitted by the data subjects per email on 30 September 2024. A confirmation of receipt was provided on 3 October 2024, acknowledging the request and outlining the next steps: *"We can confirm we have received your request and will respond as soon as possible, in any event no later than one month from your request."* Subsequently, a preliminary response was issued, and part of the requested data, compiled into a DSAR pack together with applicable legal documentation, was returned to the data subjects on 30 October 2024. The compressed folders with the returned data were password protected, and the passwords were sent in respective separate emails. Adobe indicated they needed additional time to provide information contained in application logs. As reason for the delay they stated the scale of their infrastructure and *"our attempts to search through them for individual data points relating to you specifically as an individual has required us to build new automations to navigate the larger clusters designed to ensure we are searching every potential location"*.[147] Adobe indicated they needed no more than 32 working days to deliver the remainder of the information and delivered a second DSAR response on 13 December 2024. These additional files were shared using Adobe Creative Cloud and were not attached directly to the emails.

The contents of the responses to the DSARs are summarized in Section 2.4.3 and discussed in Section 2.4.4.

2.4.3 DSAR responses

The first DSAR responses, received on 30 October 2024, were categorised by Adobe in the following sections:

1. A general list of types of personal data Adobe processes.
2. Copies of personal data, categorised as:
    a) Profile Information (*"e.g., personal data in which you are directly identifiable"*)
    b) Usage and Technical Information *("in which we have identified data associated with your specific user ID"*), including:
        1. Product and Services Data (Adobe indicated no such data was available for one of the data subjects, but did not provide this information for both data subjects)
        2. Integrity Data
        3. Adobe Identity Data
3. Details of the purposes for which Adobe collects and processes each type of personal data.
4. Information regarding the categories of recipients with whom Adobe shares personal data.
5. The duration for which Adobe retains each type of personal data.
6. Any safeguards or measures in place to protect personal data during storage and processing.

The information was provided in a PDF letter providing context to the response, links to publicly available Adobe documentation and policies, and Adobe's descriptions of the returned data types. The personal data was provided in separate PDF and CSV files which will be discussed in

[147] Adobe DSAR Response, 30 October 2024, p. 1.

more detail below. PDF copies of the applicable Adobe & Student Privacy Policy[148], Privacy Policy[149] and Adobe Technical and Organizational Measures[150] were included.

The response also contained instructions as to how a user may use an online tool to download additional data from Adobe Community[151]. The tool failed to return any data to Privacy Company.

The second DSAR responses, received on 13 December 2024, reiterated some of the information from the first response and additionally provided:

a) Application logs
b) Product and Services Data
    - Product and Services Usage Data
    - Personalization@Adobe Data

The personal data was provided in CSV, Excel and PDF files, where Adobe noted that *"certain data is being presented in its raw format, which we would not normally do when handling a standard DSAR but something we assumed was not going to be an issue given your technical expertise"*.

Adobe also indicated that in some cases they did not provide all the information because exemptions were applied on a case-by-case basis, stating one of these two grounds:

- *"information that does not constitute your personal data, for example business-related information or information that relates to other individuals (the right of access gives individuals a right to their personal data only); and"*
- *"information that also relates to other individuals who have not given consent to us to provide the information to you and where it would not otherwise be reasonable to release the information to you without their consent."*

The next sections describe the provided personal data in more detail.

2.4.3.1 Profile Information

Both data subjects received two PDF files with profile information: one with information related to their personal Adobe ID and one with information related to their Federated ID. Adobe clarified:

> *"it appears from the results in your DSAR pack that you created a non-student Adobe ID that you later transformed into a student Adobe ID (meaning that more data was captured than would have been if just a student Adobe ID had been created initially). Additionally, the account you identified as being in scope for your DSAR has administrative permissions,*

[148] Adobe. "Adobe & Student Privacy Policy", URL: https://www.adobe.com/privacy/student-policy.html, Exported by Adobe 30 October 2024, Last updated 21 July 2024.

[149] Adobe, "Adobe Privacy Policy", URL: https://www.adobe.com/privacy/policy.html, Exported by Adobe 29 October 2024, Last updated 18 June 2024.

[150] Adobe, "Technical and Organizational Measures", URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/TOMs-2021DEC2.pdf, Exported by Adobe October 2024, Published 2 December 2021.

[151] Adobe Community, "Settings", URL: https://community.adobe.com/t5/user/myprofilepage/tab/personal-profile:personal-info#, Last viewed 5 February 2025.

meaning again that the personal data identified as being associated with your account is not typical of a student Adobe account (and is instead more indicative of an Adobe account with administrative permissions for educational products). This combined with the fact that we found both "Federated ID" information (e.g., profile information about you as a user that is created, owned and managed by the organization) and Adobe ID information (e.g., created owned and managed by the end user as an individual) means that there are two sets of information in certain categories, and we have identified each when relevant."

All PDF files begin with a summary of the user's account information, opt-in/opt-out marketing preferences, description of data available elsewhere, and references to later addendums. The highlights of these documents are listed below. Full information on the content of these files is available in Section 6 of the Technical Appendix.

This 'Service Accounts' addendum contains the user's current IP address and the first date during which this IP address was documented by Adobe. As described by Adobe, this section *"describes the services (including those services that have been cancelled or terminated) that are associated with your AdobeID. Adobe also retains the last five login in IP addresses for anti-fraud purposes"* This addendum also contains tables listing Adobe services and whether or not they are active for the user. Finally, the addendum contains a table of downloaded Adobe products and a list of products (including web-based products) used by the data subject.

The 'Customer Care Case Notes & Email Activity' addendum contains a table summarizing emails sent from Adobe services to the users in addition to the full text of these emails. Where the current user is in an administrator role, this data includes the names and emails of users who sent requests for access to shared documents or access to specific Adobe services.

Limited *'Engagement tracking'* information was provided for some profiles, showing tutorials users had viewed in Adobe applications.

The responses for the personal accounts contain similar information. Additionally, for personal accounts the following information was provided:

- Additional user registration information:
    - The country in which the user lives
    - The user's month and year of birth
    - The IP address used by the user during registration
- Basic analytics ('search executed' + timestamp') for Adobe's educational resources
- Basic targeting information in the marketing database, consisting of:
    - Customer type
    - Business
    - Group
- Adobe Sign profile information

2.4.3.2 Integrity Data

Both data subjects received CSV files containing data about license integrity information for Adobe's desktop applications. Of note in this data is the following:

- The data contains a unique operating system user identifier. Privacy Company cannot confirm if this ID is taken from the OS or is calculated in some way by Adobe.

- OS system information is included (type, version, etc).
- Internet service provider information and IP addresses are included.
- Hostname and workgroup information are included.
- One of the data subjects was identified as 'enterprise user', the other wasn't. Adobe clarified that *"This value in this field is inferred data, intended to detect if a user is a consumer, or an enterprise user. Adobe is currently experimenting with the ability to infer this information and is aware that it is not yet always accurate. While Adobe works to improve the accuracy of this data, Adobe is not relying on the inferred data in this field for any purposes and instead relies on licensing and contract data to confirm if an individual is an enterprise user or not."*[152]
- The SMBIOS ID of one data subject was collected, which is a unique identifier of the PC of the user. For the other data subject this identifier was not collected. This is likely a difference between users using Windows and MacOS machines.

2.4.3.3 Adobe Identity Data

Both data subjects received data containing authentication logs from Adobe identity services in a CSV file. These files contain the following information:

- Timestamp
- User ID
- Action, like:
    - Login request
    - Login successful
    - Phone number added
    - Password reset
    - Challenge solved
    - Session extended
- Email
- Username
- Country
- First and last name
- Parameters, including:
    - Date of birth (during account setup for Adobe IDs)
    - User agent / browser
    - IP location (latitude/longitude/city)
    - Requested path
    - Debug and session identifiers

2.4.3.4 Product and Services Usage Data

One of the data subjects received two CSV files titled "Product and Services Usage Complete" and "Product and Services Summary". These files contain records of users' usage of Adobe products. These files do not contain personal data specifically relating to a user besides IP address, software versions, and device information that can constitute unique identifiers. They consist of a summary of actions taken in Adobe web and desktop applications (for example: opened application) together with timing information. The returned information aligns with the information discussed about telemetry in Section 2.3.1.1, although not all information seems to

[152] Email Adobe to SURF, 13 December 2024.

be present (e.g., the technical appendix mentions an event on the 11th of September 2024, but no events for this date are present in the DSAR response).

The other data subject did not receive such usage data, presumably because the *"user has installed software applications but has not actually used them."*[153]

2.4.3.5 Personalization@Adobe Data

In addition to this PDF, each user received three PDF files relating to "Personalization@Adobe Data". Adobe provides the following description of this data:

> *"Personalization@Adobe is a system that consolidates user profile information and product licensing information for use in personalizing messaging to those users. For example, understanding that a user has a license for Adobe Photoshop, and using that information to display an in-product (in-product can mean web, mobile, or desktop) banner highlighting new Adobe Photoshop features. Other examples include messages for new users to help them better use Adobe products, or messages containing tutorial information. The use of profiles may include marketing activities but is not limited to marketing. Please note that a user with multiple account types will have a personalization profile for each identity. This is because their use of Adobe products will vary across personal and organizational use, which may affect the type of messaging they see."*

This data is used to market Adobe's first party services. The PDFs contain exports of Adobe's internal system for tracking this marketing. Privacy Company notes the following about this data:

- This data contains a list of segments (represented as numbers) into which the test users have been classified. However, Adobe does not provide a description of the meaning of these segments or the user characteristics used to assign them.
- This data contains predictive scores for each user, and a ranked percentile into which the user has been sorted. However, Adobe does not provide a description of the meaning of these percentiles or the user characteristics used to assign them.
- The data contains a list of marketing campaigns the user has been assigned to. These campaigns are represented as numbers. Adobe does not provide a description of what these numbers represent.

Adobe clarified:[154]

> *"Regarding your comment about not being able to interpret segment and campaign identifiers, even campaign and segment names follow an internal naming convention and would not be meaningful to end users, for example 'Express Management Enterprise v7 12e' or 'Account Menu Local – AM (T1)'. Also, due to prioritization between campaigns and additional filtering (including marketing opt-outs) being applied, a user being present in a campaign or segment does not mean they would receive that specific campaign experience."*

[153] DSAR response 30 October 2024, p. 7.

[154] Email Adobe to SURF 28 March 2025.

Regarding K-12 users, they clarified:

> *"If any campaigns were categorised as marketing, additional downstream suppressions are in place designed to ensure marketing doesn't occur for known K-12 students or young users."*

2.4.3.6 Application logs

With the second DSAR response, both data subjects received a ZIP file containing application logs. The ZIP file contained numerous CSV files with raw logging data that seems to originate from several Splunk[155] clusters that centrally process Creative Cloud and Document Cloud log entries. The files were the same for both data subjects, Adobe clarified:

> *"In the case of some application log data, we have combined your results with [the other data subject (red. Privacy Company)] given the identification of this data was only something we could identify as being associated with your specific Adobe IDs by running complicated cross-referencing procedures that we do not conduct as part of our day-to-day operations (meaning that but for your requests, these categories of data would not have been identified as relating to either you or [the other data subject (red. Privacy Company)] individually)"*

The shared log files contain log entries from the 1st of August 2024 till the 21st of November 2024 and in total 58426 log entries were provided. Log entries are available for all days where test scenarios were conducted.

The logs contain entries from Adobe Acrobat, Adobe Sign and Adobe Express. Other products are not included. The contents of the logs seem to hold typical data: request details, IP address, user identifier and/or user email. Sometimes, a file name of an opened document was logged. No special categories of personal data or more detailed content data were observed. No non-Adobe URLs were found in the log entries. Some of the entries point at automated virus scans for documents.

Based on the filenames and Splunk server names, the logs seem to be stored in Splunk environments in the EU and US. Most of the log entries, about 96%, seem to be stored in the US. The log entries seem to have been selected by searching for all entries with the relevant usernames and/or user identifiers.

Some log entries contained the file name of documents stored locally by the user that were opened in the Adobe Acrobat desktop application but were never uploaded to the Adobe Cloud Storage. These log entries contained references to the Acrobat cloud preferences saving mechanism discussed in Section 3.2.7.3. These log entries were stored in the US. Adobe clarified that this issue will be fixed in a future release:[156]

> *"This was an unintended effect of an Adobe Acrobat feature, which will be fixed in an upcoming release so that the file path and name is no longer captured in logging data. Specifically, this was caused by a feature that supports checkmarks in the comments panel, which is backed by a preference that is maintained locally as a registry entry. Adobe stores the file name in the registry, and this entry is currently stored in a registry*

[155] See www.splunk.com.

[156] Email Adobe to SURF, 4 April 2025.

hive that is synced across all user's devices, which reason for the registry entry (and the file names in the registry) to be logged. This registry will be moved to a privacy section, and the file names and paths will no longer be logged."

Update after completion of Part A

Regarding the file names of locally stored files that were logged Adobe stated: "*This was not expected behavior and Adobe developed and released a fix and released it in April 2025.*"[157]

The traffic to Adobe Sign seems to involve the retrieval of 'agreements' from the Adobe Sign environment, even though the current test users did not have an Adobe Sign license and couldn't use Adobe Sign. Adobe clarified that this is due to use of the Adobe Acrobat eSign capabilities:[158]

"This traffic is related to your use of Adobe Acrobat eSign capabilities, such as the Fill & Sign Acrobat native tool. When eSign capabilities in Acrobat are used, Acrobat will call the Fill & Sign server, which in turns calls Adobe Sign to perform the actual signing operations."

2.4.4 Discussion

An analysis of the DSAR responses leads to the following observations:

1. Adobe seems to store fewer personal data types for Enterprise/Federated IDs than for Adobe IDs, in line with their privacy guarantees.
2. Application logs were only provided for a subset of applications. It is unclear whether for the other applications no logs are present or if Adobe could not provide these log files.
3. Most application logs seem to be stored in the US.
4. Log entries seem to have been selected by user identifier and username. Due to this selection process, not all relevant log entries may have been captured (e.g., in some cases users could only be identifiable by their IP address or unique cookie identifiers).
5. The Adobe preference saving functionality, which is enabled by default (see Section 3.2.7.3), can cause the file names of locally stored files to be logged and stored to the Adobe Cloud.
6. At several places, unique device identifiers are stored and used by Adobe, for instance in the license integrity systems.
7. No personal data from third-party services were provided, even though in Section 2.3.2 several third parties were identified that handle requests for Adobe, including identifying cookies.
8. Not all personal data can be properly interpreted by Privacy Company. An example of this is the Personalization data for which meaning of the segment and campaign identifiers is unknown.
9. In some cases, Adobe points users to other tools to access their data. An example of this is the online data download tool for the Adobe Community.

[157] September 2025 Response to SURF Concerning Technical Mitigations (4 Oct 2025).

[158] Email Adobe to SURF, 4 April 2025.

10. Not all collected telemetry data seems to have been returned in the DSAR response. This could either be because this data was already deleted or anonymised, or because the DSAR response is incomplete.

In response to version v0.5 of this DPIA, Adobe stated they provided all available and responsive application logs for the applications that were in scope for the DPIA. *"Regarding telemetry data, Adobe provided all telemetry data collected for product improvement purposes for the applications that were in scope. For Adobe Express, there was no telemetry data for product improvement collected for the user IDs of the accounts used for testing. This may be because users in the Netherlands are automatically opted out of non-essential cookies, and the accounts used for testing did not opt in."*[159]

3 Privacy Controls

This Section 3 discusses the available privacy controls for administrators and end-users to influence the processing of personal data, and the processing of personal data through other parties, including external apps, as well as other controls. This section also describes the *default* settings of such controls, and situations where admins do not have central privacy controls.

3.1 Privacy controls for admins

This section describes twelve different privacy controls system administrators can exercise:

1. Organisation settings
2. User and authentication management
3. Product management
4. Package management
5. Storage
6. Projects
7. Sharing restrictions
8. App integrations
9. Add-ons policy
10. Custom font management
11. Content logs
12. Audit logs

These options are discussed in more detail below.

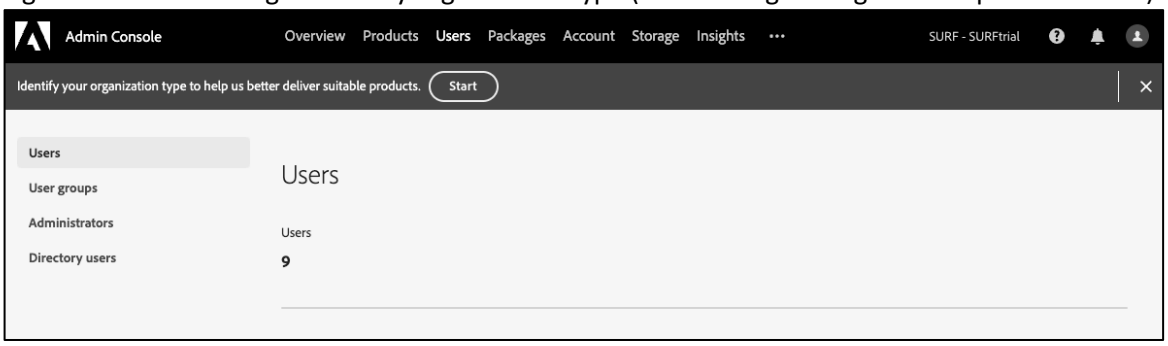
3.1.1 Organisation settings

The Admin Console prompt users to identify their organisation type (see Figure 3), offering a choice between K-12, higher education and non-profits (see Figure 4). Although the dialog shows this as a *'required action'* and Adobe has indicated in response to questions that this is a *"a mandatory segment survey"*[160], during testing it was possible to ignore the dialog. The tests performed for the purpose of this DPIA have thus been concluded without making an explicit choice.

[159] Feedback Adobe 18 December 2025.

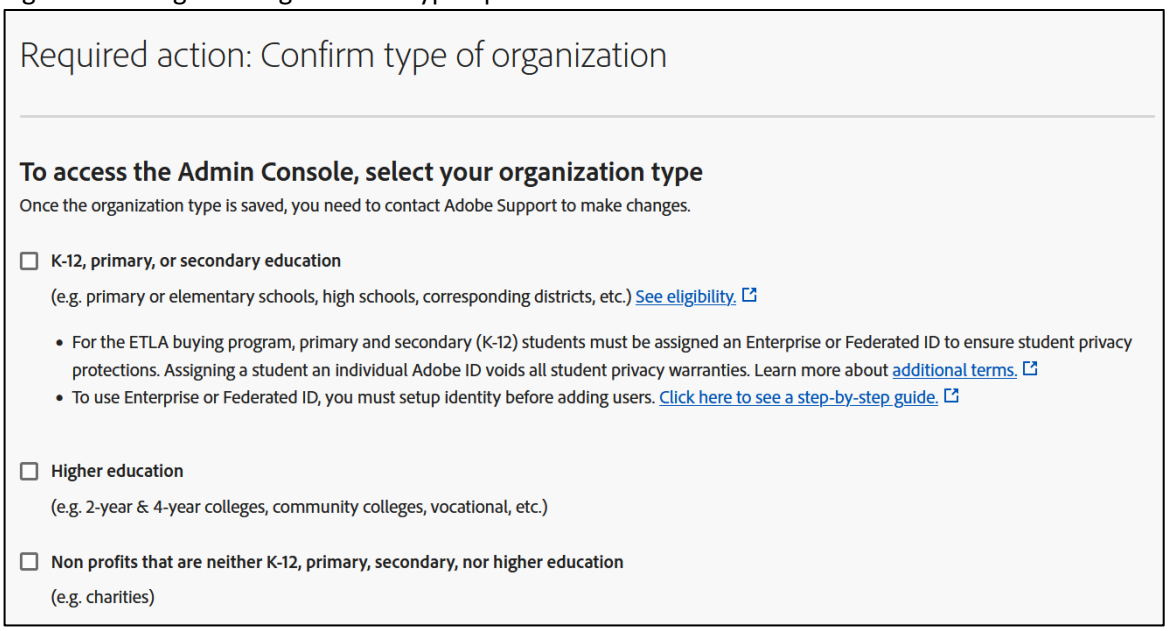
[160] Email Adobe to SURF of 17 January 2025.

Figure 3: Banner asking to identify organisation type (seen during testing on 24 September 2024)



Adobe later clarified that: *"The organisation sub-segment designation step in the Admin Console was made mandatory as of November 2024 and can no longer be skipped."*[161]

Figure 4: Dialog with organisation type options



After selecting the organisation type, this is shown on the page *'Account'* > *'Organization Details'* (see Figure 5). The value is static and can only be changed by contacting Adobe Support.

According to Adobe, the selection *"leads to user profiles inheriting the tag"*.[162] Next to this selection, some integrations can be used to identify the specific type of users (e.g., student or staff member). Of these integrations, Adobe only mentioned 'roster sync', a feature that is only available to K-12 customers in the United States. If the exact user role or education type is not available, Adobe assumes users are students.[163]

The organisation subsegment and user role influence some of the data processing by Adobe. Adobe indicates that they opt-out users of marketing communications if they are marked as

[161] Email Adobe to SURF of 28 March 2025.

[162] Email Adobe to SURF of 17 January 2025.

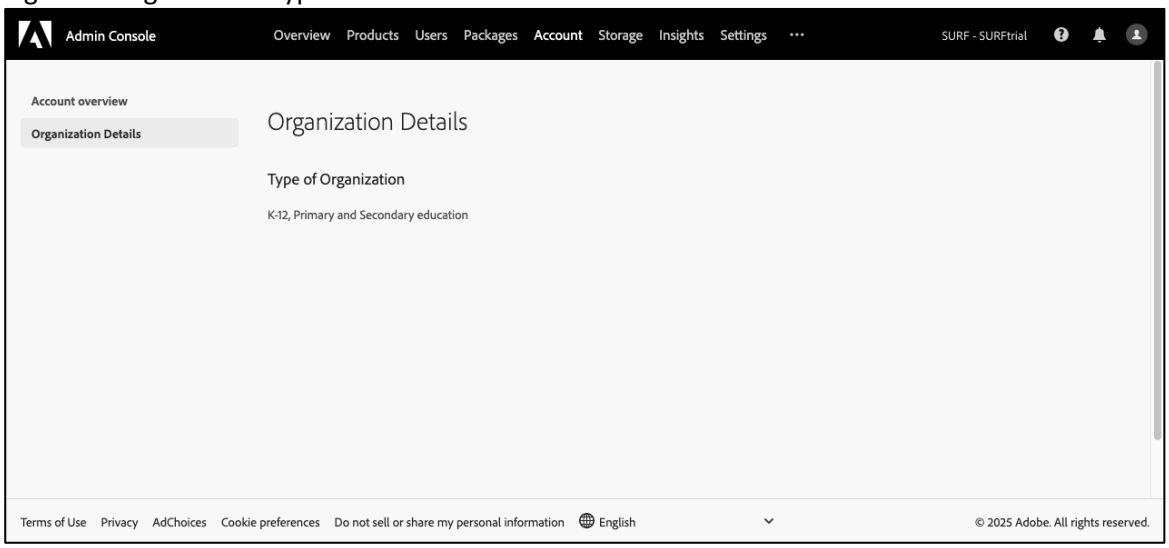
[163] Email Adobe to SURF 28 March 2025.

students. In all cases, Privacy Company was still able to opt-in to marketing mailing lists but did not receive emails in all cases (see Section 3.2.2.2 for details).

Availability of product features, on the other hand, is determined by the license entitlements assigned to users. Thus, if a K-12 user is assigned a HED license, they will still be able to access Behance and Portfolio, even if these features are meant to be unavailable to them. [164]

Availability of Adobe Stock is also based on license entitlement. For K-12 licenses, users are unable to access the Adobe Stock website directly and a curated set of Stock content will be available to K-12 users in Adobe Express.[165]

Figure 5: Organisation type shown in Admin Console



Under *'Settings'* > *'Privacy and security'* > *'Security and privacy contact settings'* (see Figure 6) the organisation can specify contact details of their:

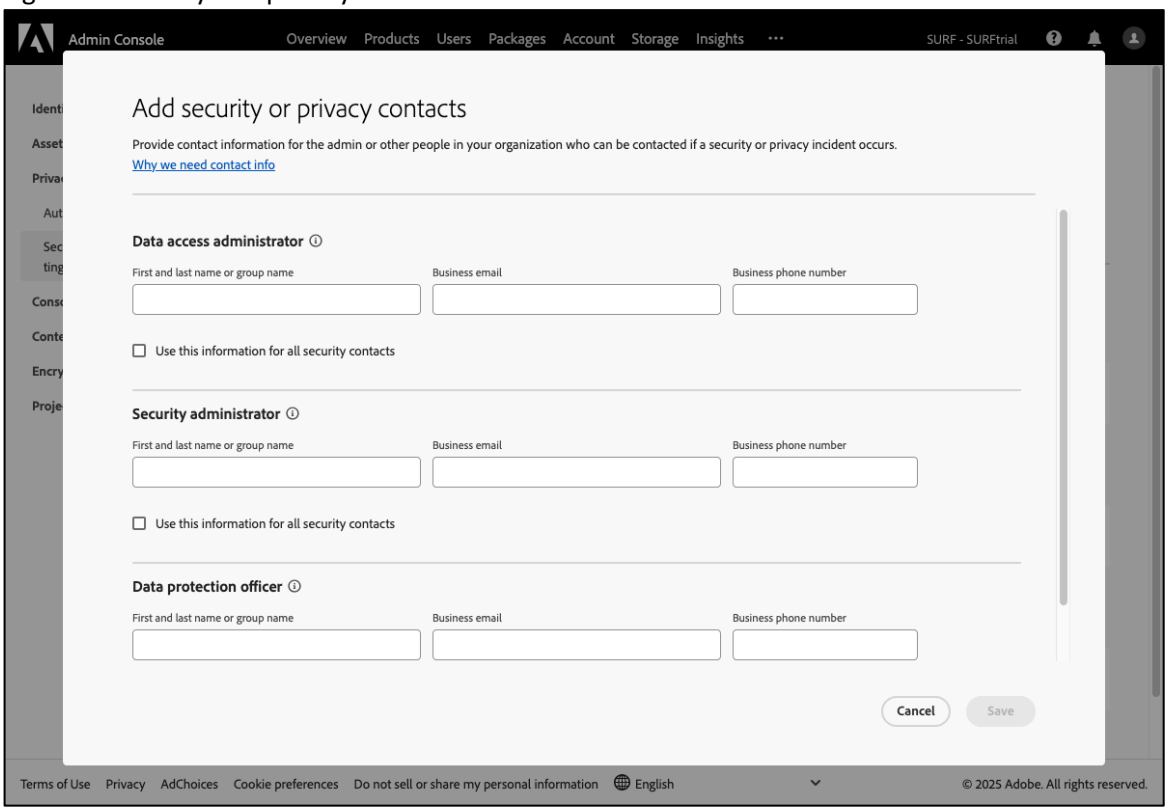
- Data protection officer (notified of privacy incidents)
- Data access administrator (notified of data subject access requests)
- Security administrator (notified of security incidents)

Adobe uses these contact details to notify the customer when required under applicable law or the terms and conditions (e.g., an article 33(2) GDPR notification).

[164] Adobe DSAR response of 30 October 2024, p. 2 and email Adobe to SURF 28 March 2028.

[165] Email Adobe to SURF of 4 April 2025.

Figure 6: Security and privacy contacts in Admin Console



3.1.2 User and authentication management

The Admin Console allows administrators to manage users and set up automatic synchronisation of users from their own identity servers. The managed options available depend on the type of user identity used. These types were discussed in Section 1.3.1.

3.1.2.1 Authentication and profiles

Over the last years, Adobe has been migrating enterprise users to their Enterprise Storage Model (ESM, also referred to as Business Storage Model or Adobe storage for business). This model is discussed in more detail in Section 3.1.5. Once an organisation has been migrated, the *'Storage'* tab becomes visible in the admin console.[166] As part of this effort, Adobe has introduced *'Profiles'* to allow users to choose between using their personal storage and product entitlements, or those of their school or workplace. After authentication, users are, when necessary, presented with a profile chooser to select the environment to work in.

Users can authenticate with Adobe IDs, Enterprise IDs or Federated IDs.[167] An Adobe ID is created and managed by the end user and is a personal account. Under the Enterprise Storage Model, this personal account is linked to the organisation by creating a *'Business ID'*. After authentication, the user can use the profile chooser to select the organisation profile. This model

[166] Storage Management after Update, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/kb/storage-management-after-update.html.

[167] Identity overview, last updated: 16 December 2024, URL https://helpx.adobe.com/enterprise/using/identity.html.

ensures that the user's personal documents and business documents are stored separately, and that the organisation maintains control over the business documents.

Enterprise and Federated IDs are fully managed by the organisation. In case of an Enterprise ID, authentication is handled by Adobe, whereas for Federated IDs the authentication is handled by the organisation using single sign-on.

3.1.2.2 User account creation and management

When using personal Adobe IDs, administrators can only manually create, update and remove these user accounts in the Admin Console, optionally using a CSV bulk upload. [168]

For Enterprise IDs, user identities can also be synchronised automatically using the User Sync tool (UST) or the User Management REST API. Federated IDs can use the Microsoft Azure Sync or Google Federation Sync in addition to these methods. These strategies allow synchronisation of the name, email address, country and group information of users.

When using Enterprise of Federated IDs, administrators first must verify domain ownership of the organisation's domain by adding the domain to the Admin Console and setting up a DNS record.[169] User accounts can then be created using above mentioned methods. For Federated IDs, accounts can also automatically be created (or updated) when a user logs in through single sign-on (for Federated IDs) or using the Azure or Google synchronisation.[170] When users are deleted from a synchronised directory, they will also be deleted in the Adobe environment.

3.1.2.3 Directory users

The Adobe Admin Console keeps track of users in separate lists per directory (in addition to the global user list). These directory user lists contain a list per configured directory, as well as a list of users that use a *'Business ID'* (like an Adobe ID linked to an organisation).

When removing a user from the Admin Console, an administrator must keep in mind that he must also remove the user from the underlying directory to fully remove the user details from the Adobe organisation. This can be done manually or by one of the automated synchronisation methods. The Admin Console user interface does not warn about the fact that user information is stored in multiple places.

In some of the documentation materials, Adobe suggests that even for Enterprise and Federated IDs a Business ID will be created: *"Since every new user Enterprise ID or Federated ID type user is linked to a business profile, the user will also be available in the Business ID directory."*[171] Adobe clarified that this is only the case if Enterprise ID or Federated ID type users have multiple organisation memberships.[172] This means that, for some cases, to fully remove an Enterprise or Federated ID, the administrator will have to remove the user in three places: the list of users, the Business ID directory users and the domain's directory users. In the test environment this

[168] Adobe Admin Console users, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/users.html.

[169] Add domains to directories, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/add-domains-directories.html.

[170] Enable automatic account creation, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/automatic-account-creation.html.

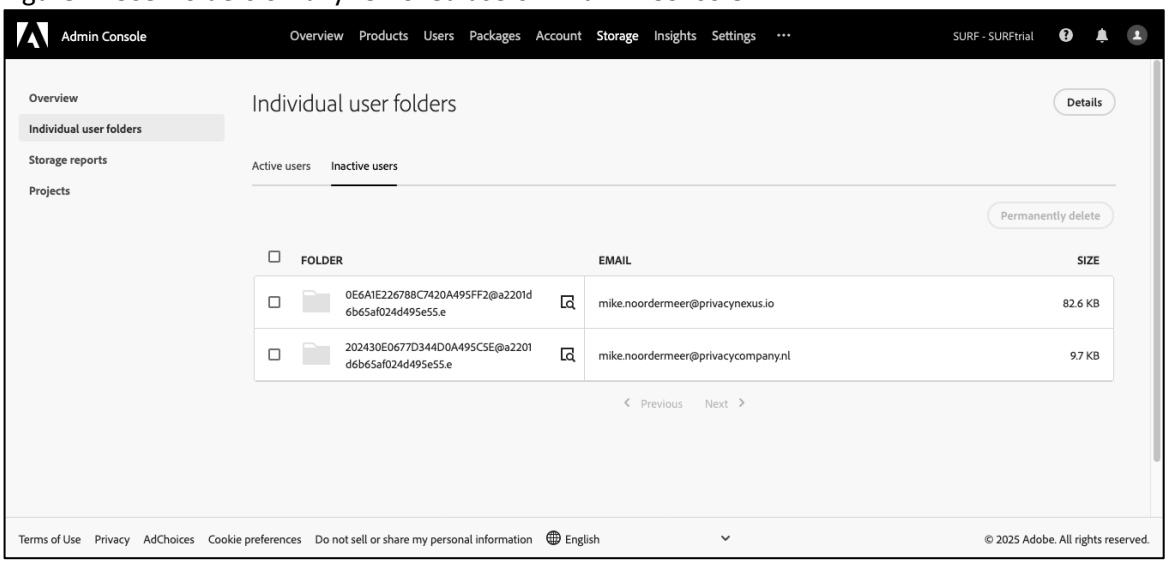
[171] Manage directory users, last updated: 18 April 2023, URL: https://helpx.adobe.com/enterprise/using/manage-directory-users.html.

[172] Email Adobe to SURF, 4 April 2025.

duplication only occurred for one of the directory users, the other directory users were only listed in the domain's directory.

Note that fully removing a user does not seem to remove the assets of a user, although Adobe does give that impression in some of their documentation.[173] After fully removing the user, the user was still listed in the list of 'inactive users' and the assets could be reassigned to another user. The username was changed into a random identifier, but the email address was still present (see Figure 7). After several months, this email address was also removed and replaced with a random identifier.

Figure 7: User folders of fully removed users in Admin Console



3.1.2.4 Domain enforcement

Administrators can enable *'domain enforcement'* on the organisation's verified domains. This feature prevents users from creating and using personal Adobe IDs on the organisation's domains.[174] Domain enforcement is enabled by default on newly created Enterprise and Federated directories. Existing users with an Adobe ID can either be migrated to an Enterprise or Federated ID (see the next section) or can be required to change their email address to a domain not owned by the organisation. Specific Adobe IDs can be excluded from domain enforcement.

3.1.2.5 Identity type migration

When deploying Enterprise of Federated IDs, administrators have the option to migrate existing Adobe IDs to Federated or Enterprise IDs. It is also possible to migrate existing Enterprise IDs to

[173] One page mentions *"If you permanently delete users, the user is removed along with all the Creative Cloud assets belonging to that user. The user and the assets then can't be recovered"* (https://helpx.adobe.com/enterprise/using/manage-directory-users.html) but another only says *"If you remove Directory Users for security reasons, all references to the user's name and email address are removed. Only a unique alphanumeric ID is retained in the Admin Console. When you reclaim such assets later (…)"* (https://helpx.adobe.com/enterprise/using/manage-users-individually.html).

[174] Domain Enforcement for restricted authentication, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/restricting-domains.html.

Federated IDs or vice versa (e.g., when introducing or removing single sign-on).[175] Migration maintains the user's content and access level.

Migration from an Enterprise to Federated ID, or vice versa, is fully automatic. For migration from an Adobe ID, the administrator needs to upload a CSV file with the users to be migrated and the new identity type. The user is asked in an email to login and then asked to consent to an automatic transfer of all their assets to their new business profile (assuming certain preconditions are met, see the documentation for details). If the user does not consent, no content is transferred, and they will have to manually transfer their document to the business profile. To automatically migrate assets, the Adobe ID and the new Enterprise or Federated ID need to be located in the same storage region.[176]

To see what users have a personal Adobe ID with the organisation's domain, the administrator of the domain can generate a report through *'Insights'* > *'Reports'* > *'Personal accounts of managed domains'*. The report only lists Adobe ID users that have accepted the latest version of the Terms of Use.[177]

3.1.2.6 User groups

User groups can be defined through the Admin Console or synchronised from the organisation's directory.[178] User groups can be used to assign licenses to multiple users at once but cannot be used to assign administrative permissions. User groups can be administered by designated Group Administrators.

3.1.2.7 Authentication settings

For Adobe and Enterprise IDs, administrators can set additional authentication requirements on the *'Settings'* > *'Privacy and security'* > *'Authentication settings'* page (see Figure 8), including:

- A password policy (strength and expiration)
- Enforcing 2-step verification
- Disallowing social logins through Facebook, Apple or Microsoft (only applicable to Adobe ID accounts)
- Setting a maximum session lifetime and idle time

All these settings are not applicable to Federated IDs, where the single sign-on provider is expected to enforce such authentication policies.[179]

[175] Edit user identity type, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/switch-user-identity.html.

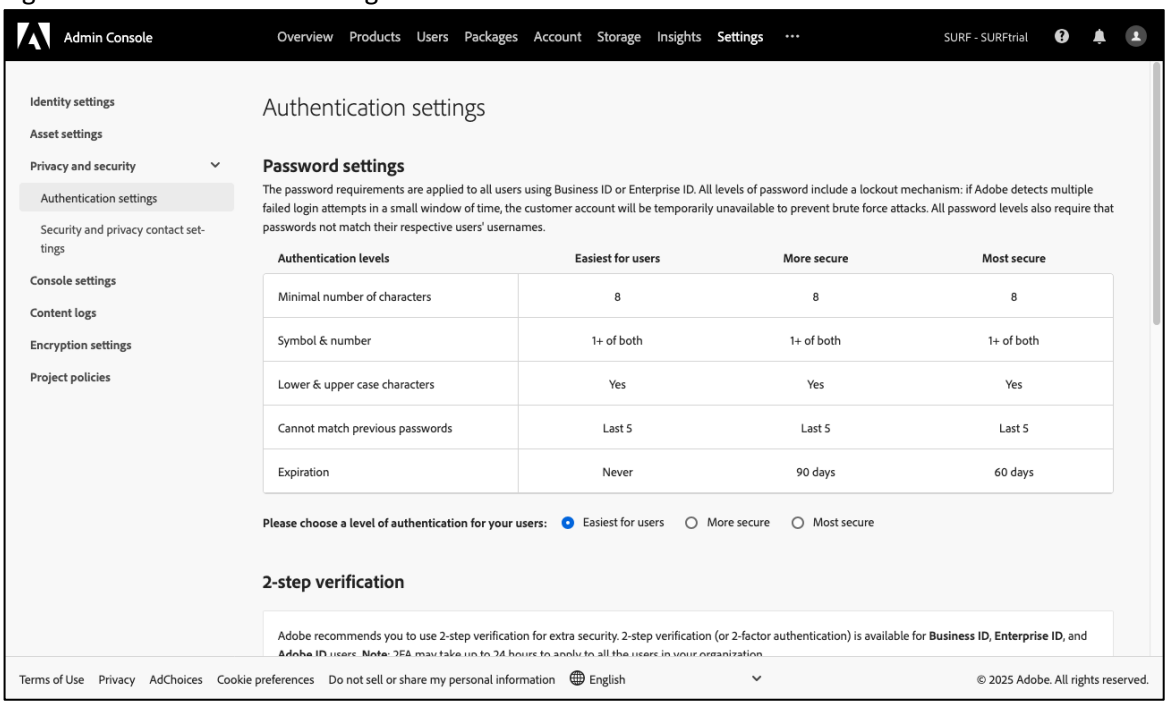
[176] Automated Asset Migration FAQ, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/asset-migration-faq.html.

[177] Domain Enforcement for restricted authentication, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/restricting-domains.html.

[178] Manage user groups, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/user-groups.html.

[179] Authentication settings, last updated 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/authentication-settings.html.

Figure 8: Authentication settings in Admin Console



3.1.2.8 Administrative roles

Administrators are managed through the Admin Console and are regular users with additional administrative roles assigned to them. Such users can use any identity type, although the primary administrator always uses and Adobe ID for emergency access.[180]

Administrative roles are available in a hierarchy: next to system administrators having full system access, there are also product-specific administrators, support administrator, storage administrators, et cetera.[181]

3.1.3 Product management

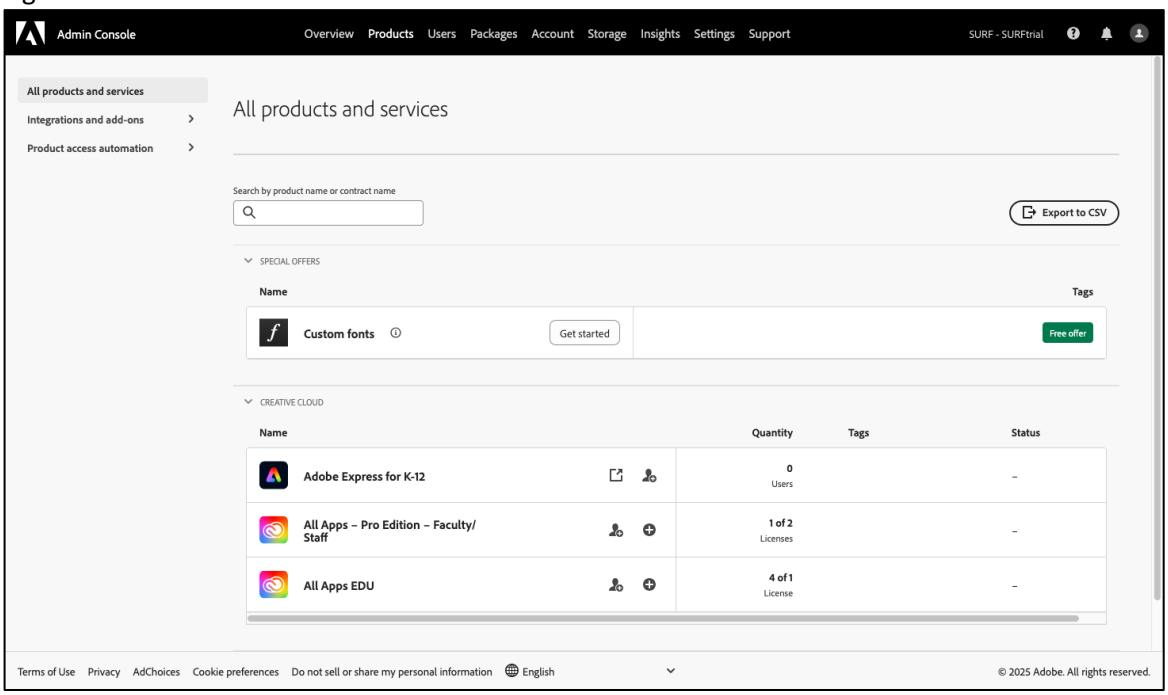
The Admin Console lists the available products on the *'Products'* tab (see Figure 9). A product can be a single application (e.g., 'Photoshop') or a plan consisting of multiple applications (e.g., 'Creative Cloud All Apps').[182] Each product has one or more 'product profiles' defined, that allow specifying optional services and self-service policies for the profile (see below). Product profiles are assigned to users to give them access to applications.

[180] Email Adobe to SURF of 9 January 2025.

[181] Administrative roles, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/admin-roles.html.

[182] Manage products on Admin Console, last updated 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/manage-products.html.

Figure 9: Products shown in Admin Console



3.1.3.1 Product assignment

Products are made available to users by assigning a product profile to the user. There are several ways to do this:

- Assign the product profile directly to the user
- Assign the product profile to a user group the user is a member of
- Use an automatic assignment rule
- Use product requests

An automatic assignment rule will provide the administrator with an URL that they can communicate to users to automatically assign themselves a product. Optionally, it allows users to self-assign the product from the Creative Cloud desktop and web application. The selection of users can be scoped to a specific directory or domain.[183]

Product requests allow end-users to request access to Adobe products and services. The requests are shown in the Admin Console and an administrator can review these requests and grant or deny them. Product requests are enabled by default but can be disabled by an administrator.[184]

Depending on a setting in the product profile, users will be notified through email when they are added or removed from a product profile.[185] Note that new Adobe or Enterprise ID users will always receive an email on their first assignment, as they will have to setup their account. When

[183] Manage automatic assignment rules, last updated 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/automatic-assignment-rules.html.

[184] Manage product requests, last updated 10 January 2025, URL: https://helpx.adobe.com/enterprise/using/product-request.html.

[185] Manage product profiles for enterprise users, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/manage-product-profiles.html.

removing a product assignment, some Adobe products email users to keep their data available (e.g., Adobe Portfolio emails a user to update their plan, in order not to lose content).

3.1.3.2 Optional services

Each product profile allows the administrator to configure the available services (see Figure 10).[186] Only optional services can be disabled and certain core services are always enabled, including Storage, File Syncing, Sync Settings, Collaboration, Creative Cloud Libraries and Color CC. Adobe lists the optional services on a web page[187], but during testing other services were listed as optional services in the product profile as well.

Some notable services that can be turned off are:

- Adobe Express
- Adobe Sign
- Photoshop online
- Fonts
- PDF Services (enables certain PDF operations in Acrobat that require data processing in Adobe Cloud; Adobe refers to this optional service as 'essential')
- Community (Behance) and Adobe Portfolio

Although '*Frame.io*' is listed on the Adobe web page as optional service and a link to Frame.io is displayed in the Creative Cloud desktop and web application, it is not possible to disable Frame.io in the product profiles.

For the product *'Adobe Express for K-12'* it was possible to disable the *'Adobe Firefly'* service.[188] When disabled, accessing the Firefly website displays an error (see Figure 11) and Firefly-based features are not available in Adobe Express. Disabling Firefly was not possible for the complete *'All Apps'* products.

[186] Enable/disable services for a product profile, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/enable-disable-services.html.

[187] Optional services, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/optional-services.html.

[188] Adobe Firefly generative AI features for K12, last updated 16 December 2024, URL: https://helpx.adobe.com/enterprise/kb/adobe-firefly-for-k12.html.

Figure 10: Product profile service selection

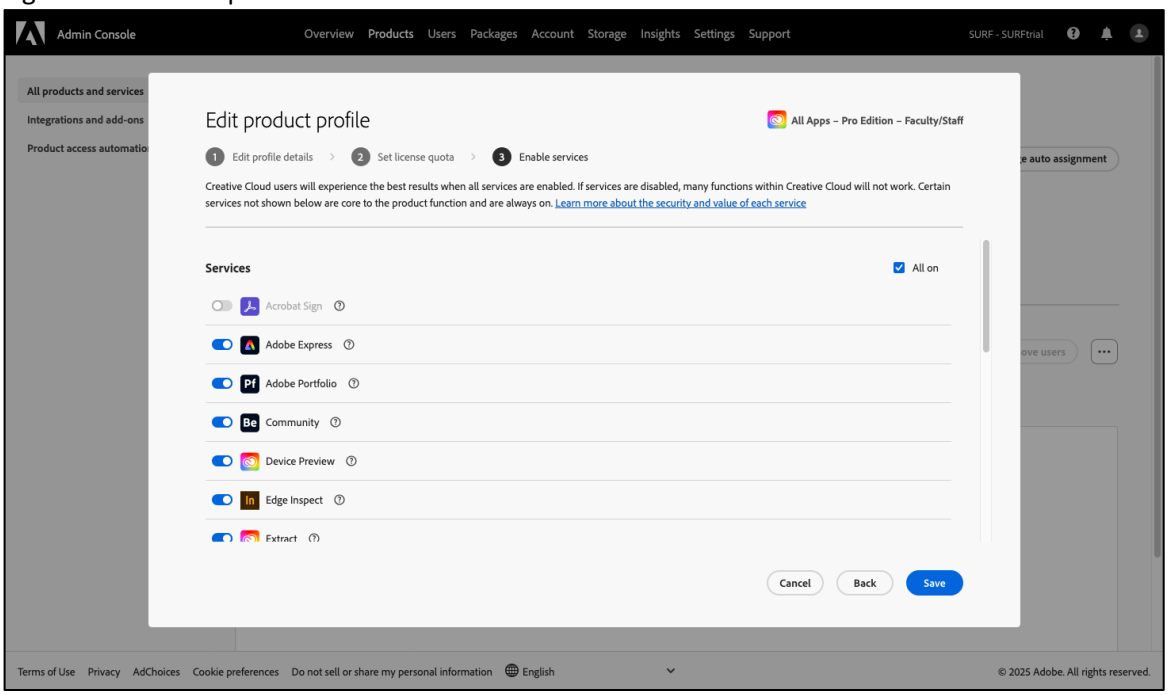
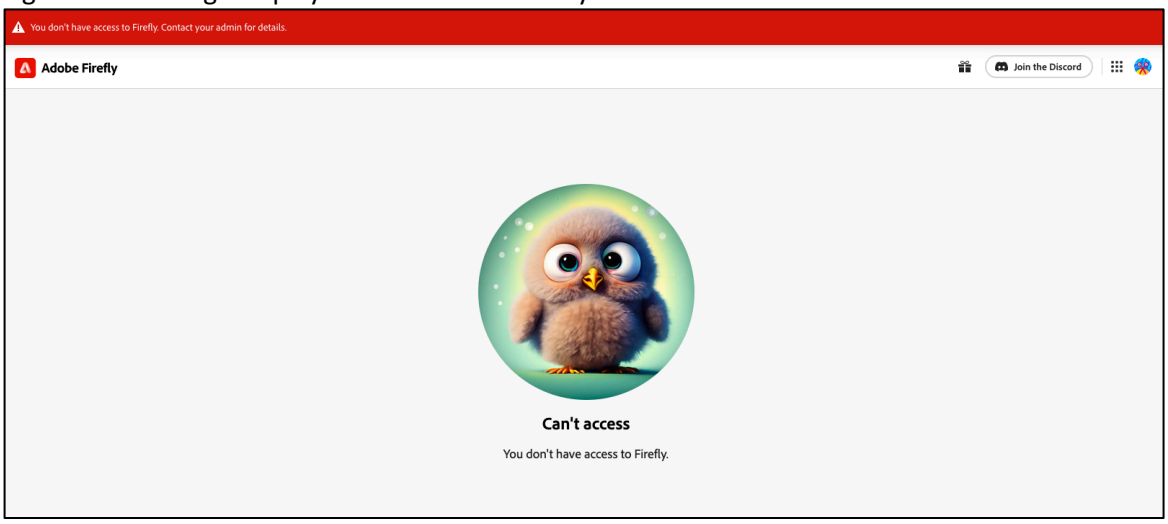


Figure 11: Message displayed when Adobe Firefly has been turned off



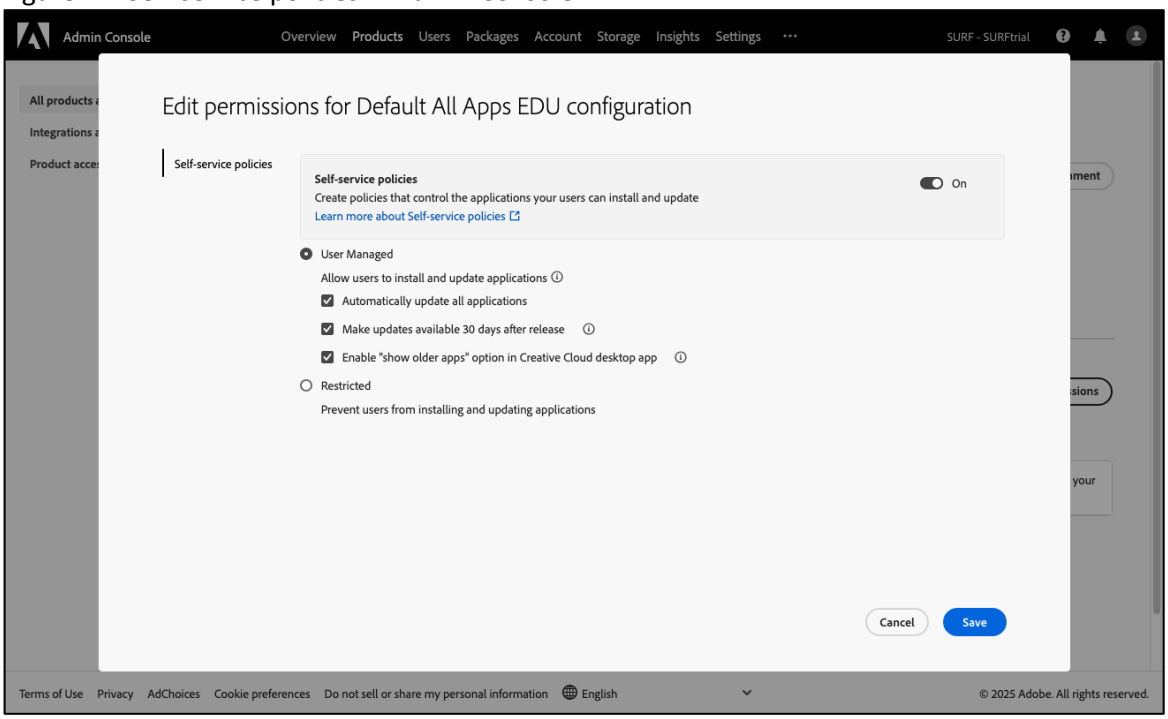
3.1.3.3 Self-service policies

Administrators can set a self-service policy for a specific product profile (on the *'Products'* page, choose a product, choose a profile and then choose *'Permissions'*, see Figure 12). The self-service policy controls whether users can install and update applications through the Creative Cloud desktop application. [189] Using the setting, administrators can prevent users from installing any applications themselves, forcing the use of managed packages (discussed in Section 3.1.4).

[189] Manage self-service policies, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/manage-self-service-policies.html.

During testing, restricting self-service also restricted access to the 'Discover' tab in the Creative Cloud desktop application, a restriction that was not mentioned in Adobe's documentation. Adobe has since clarified that this is intentional and updated the documentation.[190] Even when restricted, users were still able to install plugins (see Section 3.2.7.4).

Figure 12: Self-service policies in Admin Console



3.1.4 Package management

In the Adobe Admin Console, it is possible to define and download software packages. These packages install either the Creative Cloud desktop application ('self-service', giving elevated privileges to the user to install other applications) or one or more specific applications ('managed'). Pre-generated packages for individual Adobe applications (e.g., a single package containing the Creative Cloud desktop application and Photoshop) or templates (e.g., all web- or video-related applications bundled together) are also available.

By default, the package management features are not used as users can install applications using 'Adobe Self-Service': they download the Creative Cloud desktop installer from adobe.com and, assuming they have admin privileges on their system, install these applications without further restrictions. This self-service can be disabled in the product profile, see Section 3.1.3.3.

Using packages gives the administrators several additional settings:

- Specific plugins can be installed by default.
- Self-service installation, (auto-)updates, file syncing, browser-based login and beta applications can be enabled or disabled in the Creative Cloud desktop application (see Figure 13).

[190] Email Adobe to SURF, 28 March 2025.

- An internal update server can be used, reducing required network bandwidth in the organisation.[191]
- Adobe Genuine Service (AGS) can be installed together with the applications. AGS is a separate service that periodically checks if the Adobe applications on a host are genuine and notifies the user if they are not.[192] A determination by Adobe that any Adobe software is non-genuine or is unsupported may result in AGS showing messages to the Customer and/or in partial or complete inoperability, suspension, or termination of Customer's use of the non-genuine Adobe Software. [193]

Regular enterprise users are also able to disallow installations of additional plugins by the end user, but this functionality is not available to educational customers.[194] Adobe clarified that this is because *"self-service plugin installation is not available to Education customers"*.[195] Adobe also clarified this only holds for managed packages, and not for bring-your-own-devices where users use Adobe Self-Service, and recommends educational institutions to use managed packages.[196] For more information on plugins see Section 3.2.7.4.

Packages come with the disadvantage that administrators must distribute them to the users in some way, either by automatically installing the packages on managed hosts or distributing the packages manually to the user in 'bring your own device' scenarios. As students often work on their own devices, it seems unlikely that educational institutions would fully disable self-service and distribute packages manually.

[191] AUSST overview, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/update-server-setup-tool.html.

[192] Adobe Genuine Service, last updated: 30 September 2021, URL: https://helpx.adobe.com/genuine/adobe-genuine-service.html.

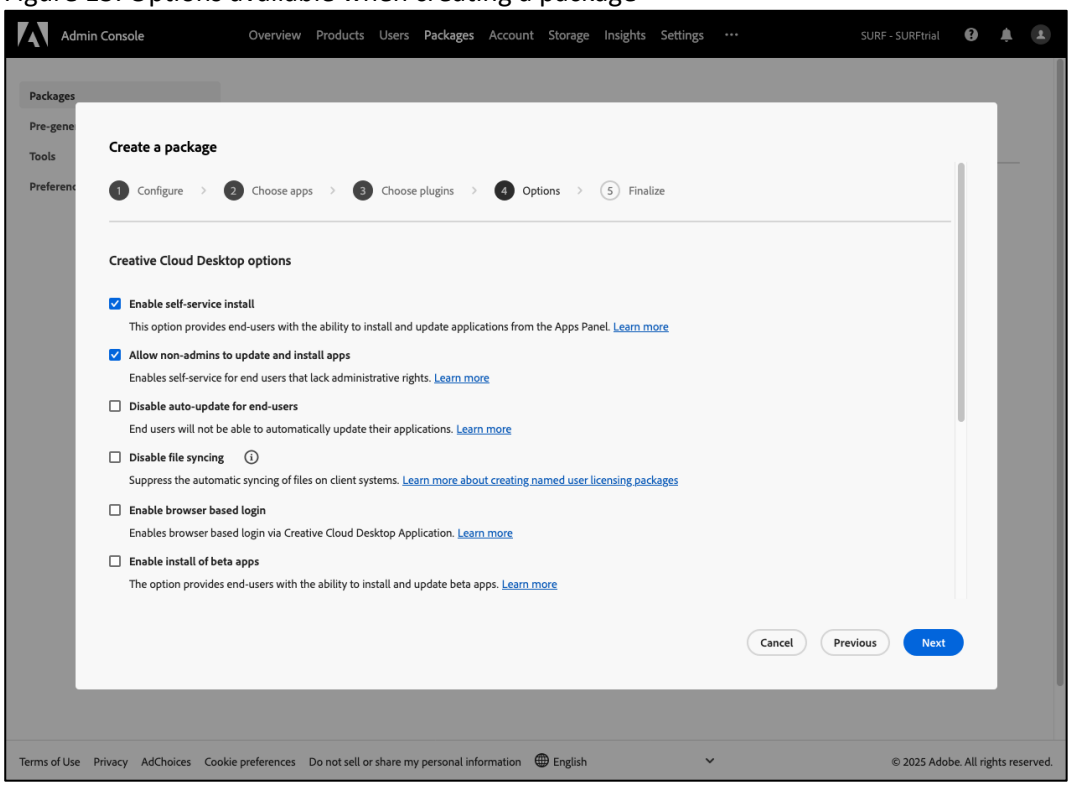
[193] Article 6, Adobe, PSLT – Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1), URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-CreativeCloudandDocumentCloudSubstance3D-WW-2023v1.pdf.

[194] Customize Adobe Creative Cloud desktop app, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/customize-creative-cloud-app.html#enable-self-service-plugin-install.

[195] Email Adobe to SURF, 14 February 2025.

[196] Email Adobe to SURF, 28 March 2025.

Figure 13: Options available when creating a package



3.1.5 Storage

Adobe has introduced their Enterprise Storage Model (ESM, also called Adobe storage for business or Business Storage Model) several years ago to better separate personal assets (documents, images and other files) from business assets.[197] Under this model, a user selects a *profile* to work with after they authenticate. Subsequently, they will only be able to access applications and assets that belong to that profile. As part of this model, administrators have gained more insight into the use of storage in their organisation, can pool the storage quota between users and can reclaim user assets when they leave the organisation. The storage is *"owned by the business"*.

After introduction of the ESM, Adobe has also opted to move the storage of Document Cloud applications (e.g., Acrobat) to this central storage model (previously only used for Creative Cloud).[198] Some of these migrations still seem to be ongoing. As Privacy Company was unable to access Document Cloud documents of users as an admin, the migration of the test environment is probably still underway (see Section 3.1.5.2).

ESM does not provide a mechanism for administrators to entirely prohibit cloud data storage.[199]

[197] Introducing the Business Storage Model, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/kb/business-storage-model-introduction.html.

[198] Migration of Adobe Document Cloud to Adobe cloud storage, last updated: 22 April 2024, URL: https://helpx.adobe.com/ie/document-cloud/help/document-cloud-on-acp.html.

[199] Creative Cloud for enterprise Security Overview, October 2021, p. 5.

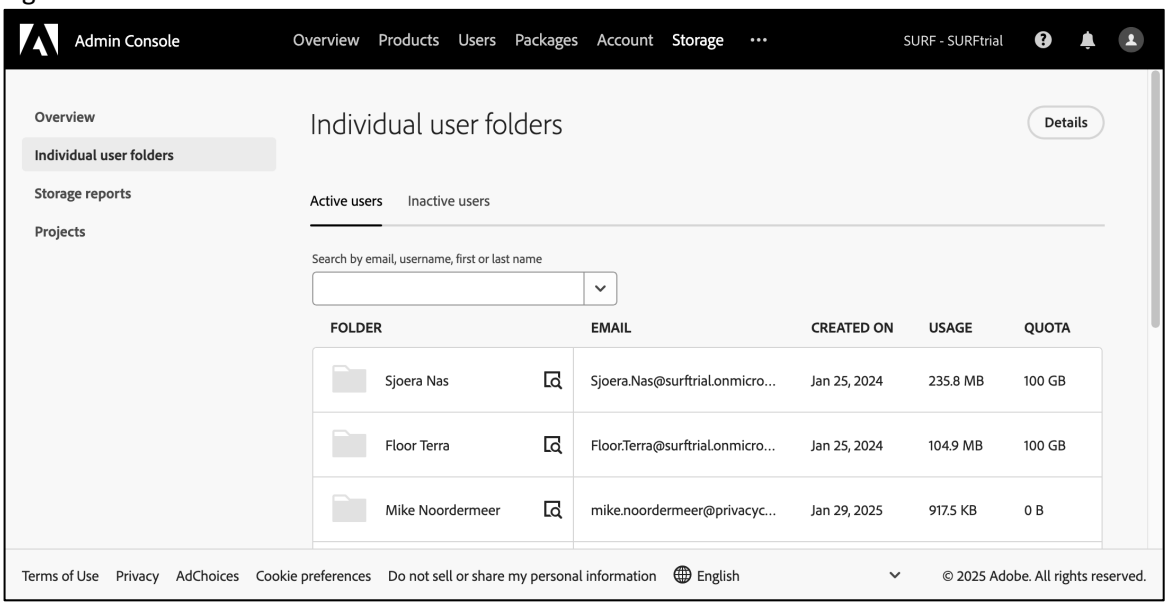
Update after completion of Part A

In August 2025, Privacy Company observed a new optional service in the product profiles: 'Enterprise User Storage'. This suggests that cloud data storage can now be disabled for users. Privacy Company did not verify the functionality of this new configuration option. Where applicable, disabling cloud data storage has been included as a possible measure in parts B-D of this DPIA.

3.1.5.1 Reporting

Administrators can view the amount of storage each users uses. It is also possible to create a CSV-report of this information, with similar data.[200] Administrators cannot directly access the information in the user's folders through these reports.

Figure 14: Overview of individual user folders in Admin Console



3.1.5.2 Accessing active user's data

In some cases, administrators may need to access files of end-users. This could, for instance, be the case when a user or legal guardian does a Data Subject Access Request (DSAR). It is unclear what features are offered to accommodate such scenarios.

The Enterprise ID documentation suggests that such accounts can be used if administrators *"need emergency access to files and data associated with a user ID"* and that *"No extra approval [is] needed"*, but does not give insight into how this would work.[201] The Creative Cloud security overview states that *"IT staff does not have direct access to any files in the user's Creative Cloud for enterprise storage"* but at the same time mentions that *"IT staff may assume*

[200] Manage Adobe storage, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/manage-adobe-storage.html.

[201] Set up organization with Enterprise ID, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/setup-enterprise-id.html.

ownership for the employee's account".[202] The Document Cloud security overview makes similar claims.[203] Adobe's legal documentation suggests that customers can contact Adobe to access student data in case of a DSAR and that *"Adobe will work with Customer and its School(s) as needed to facilitate such access"*, suggesting that there are no automated processes to access end-user data.[204]

During testing, Privacy Company noticed that administrators are able to access Creative Cloud files (Photoshop and Adobe Express) if they know the unique identifier which is used in sharing URLs (also see Section 3.2.3.2). This is also somewhat documented in the collaboration FAQ: *"When you attempt to share an asset with an administrator, you will see the message Administrators already have access."*[205] As these unique file identifiers are present in the content logs (see Section 3.1.11), administrators are able to access files without user intervention and without the user being aware of this, even though the security whitepaper claims otherwise. This method does not work for Document Cloud (Acrobat) files.

Since testing, Adobe has confirmed the ability to access to end-user files and states this is one of the ways administrators can access the files in case of a DSAR (next to asset reclamation, see Section 3.1.5.3):[206]

> *"This is by design. All content created by members of an organization using enterprise subscriptions with the Enterprise Storage Model (ESM), as seen in Creative Cloud, Adobe Express, and the latest generation of Document Cloud, is owned by the business or institution (as it is the entity paying and granting access to their members). Administrators have privileges to access any content in ESM using the correct asset ID, and administrative access and actions on stored assets are logged in the Content Logs for auditing purposes. While such direct access is possible, the Admin Console does not currently provide a method for administrators to browse and navigate directly to assets. Non-admin users in the organization who do not have access privileges to a specific asset are not able to access that asset even with the correct Asset ID (or complete sharing URL), provided the asset is not shared publicly or with everyone within the organization. "*

and:

> *"We are now requesting updates be made to the Creative Cloud for enterprise Security Overview paper. The Document Cloud Security Overview paper refers to the former Document Cloud storage, where direct access to content using an asset ID is not possible."*

For Federated IDs, where authentication is managed by the customer, an administrator could issue a password reset for an account or impersonate a user, if their single sign-on solution offers such options (this option is also suggested by Adobe in a response to SURF[207]). For Enterprise IDs, where authentication is managed by Adobe, similar features do not seem to be present.

---

[202] Creative Cloud for enterprise Security Overview, October 2021, p. 9.

[203] Adobe Acrobat with Document Cloud Services Security Overview, February 2024, p. 7.

[204] Student Data Terms, article 9.1.

[205] Collaboration FAQ, last updated: 6 October 2023, URL: https://helpx.adobe.com/creative-cloud/help/collaboration-faq.html.

[206] Email Adobe to SURF, 28 March 2025.

[207] Email Adobe to SURF, 28 March 2025.

3.1.5.3 User deletion and asset reclamation

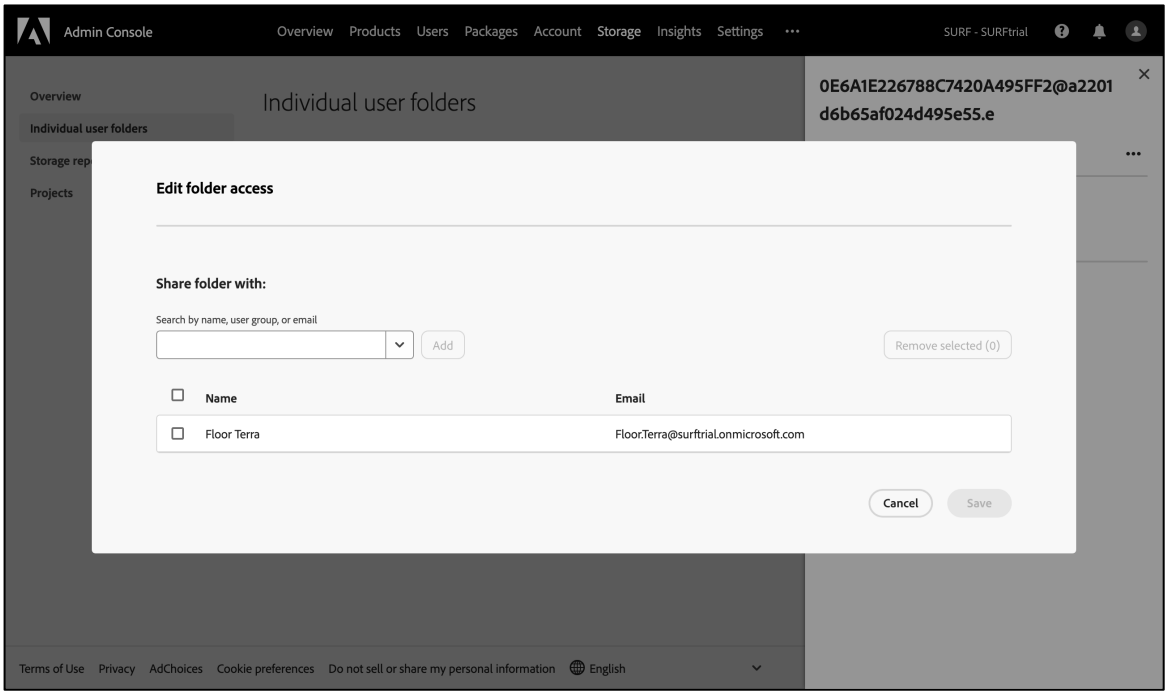
Once a user has been removed from the organisation, an administrator can choose to transfer the assets of that user to another user. For regular enterprises, this can already be done during the removal process, but for educational customers this is only possible once the user has been moved to the *'Inactive Users'* tab in the *'Individual user folders'* panel of the *'Storage'* section of the Admin Console.[208] By selecting a user folder and choosing *'Edit folder access'* the contents of the user folder can be shared with another user (see Figure 15).

When the contents of the folder are shared, the selected user should receive an email with links to one or more ZIP-archives containing the user data. Not all user data will be available, e.g., Adobe Sign agreements, Behance and Portfolio assets, and Adobe Express social posts will not be included in the archives. It is unclear if Acrobat documents are included in the archives: the asset reclamation help page suggests on one hand that reclamation is only available to users on Adobe storage for business (i.e., ESM), then states that Acrobat assets are not included for enterprise users, but continues with a statement that they *will* be included when using Adobe storage for business.[209]

Initially, when Privacy Company tried to reclaim assets from several removed user accounts, the email that should give access to the reclaimed assets was not received. This was due to a bug that since then has been fixed.[210]

While their account is still active, end-users (students or staff) can always use the Student File Transfer service to transfer their files to a personal Adobe account, see Section 3.2.3.7.

Figure 15: Edit folder access dialog in the Admin Console



[208] Reclaim assets from a user, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/asset-reclamation.html.

[209] Reclaim assets from a user, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/asset-reclamation.html.

[210] Email Adobe to SURF, 14 February 2025.

3.1.5.4 Retention period

Data of removed users is kept indefinitely and only deleted 14 days after an administrator removes the user data from the 'Inactive Users' tab in the admin console.[211]

This retention period is not readily apparent from the documentation. For instance, the Creative Cloud security overview states that data is kept for 14 days after removal of the user, but does not clarify that the user also must be deleted from the Storage section of the admin console.[212] The Document Cloud security overview states a retention period of 90 days instead, but is outdated now (most) users have moved to ESM.[213] The documentation on asset reclamation simply states that the folder of removed users is moved to the *'Inactive Users'* tab but does not state how long it will stay there.[214] And an Adobe employee states a retention period of 30 days in the Adobe community discussions, which is incorrect but this post could still be encountered by admins searching for information on the retention period.[215]

In addition to the unclear retention period, Privacy Company observed for two accounts that the user's folder remained in the list of *'Active Users'* and was thus retained, even after these two user accounts were removed from the user list. In those cases, the administrator does not have an option to force deletion of the user's folders.

3.1.5.5 Encryption

Assets are encrypted in transit using AES 128-bit GCM over TLS 1.2. At rest, the content is stored in encrypted form using AES 256-bit encryption (on Amazon S3 and EBS storage). The key management is handled by Amazon KMS (in FIPS 140-2 validated hardware security modules) with keys under control of Adobe. Keys are rotated annually.[216]

Optionally, customers can enable dedicated encryption keys.[217] This is done on an organisation-level.[218] The differences with standard encryption are:[219]

1. A unique, dedicated encryption key is generated for the organisation.
2. The organisation can revoke this encryption key (temporarily or permanently). Revoking the key makes all content encrypted with it inaccessible.
3. Students will not be able to use the Adobe Student File Transfer service to export their content to a personal Adobe ID. Due to this fact, Adobe does not recommend educational institutions to use dedicated keys.[220]

---

[211] Email Adobe to SURF, 28 March 2025.

[212] Creative Cloud for enterprise Security Overview, October 2021, p. 9.

[213] Adobe Acrobat with Document Cloud Services Security Overview, February 2024, p. 7.

[214] Reclaim assets from a user, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/asset-reclamation.html.

[215] SuJoshi in 'As an Adobe Admin, If I remove a user, how long is their adobe cloud information retained?' on Adobe Community, 16 June 2023, URL: https://community.adobe.com/t5/enterprise-teams-discussions/as-an-adobe-admin-if-i-remove-a-user-how-long-is-their-adobe-cloud-information-retained/td-p/13870563.

[216] Creative Cloud for enterprise Security Overview, October 2021, p. 6-7.

[217] Manage encryption, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/encryption.html.

[218] Dedicated encryption keys| Common questions, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/encryption-faq.html.

[219] Email Adobe to SURF, 9 January 2025.

[220] Manage encryption, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/encryption.html.

Enabling dedicated encryption does not change the key holder, encryption algorithms or security boundaries: in all cases these are managed by Adobe.

The dedicated encryption key is only used for file contents, meaning the dedicated encryption key is not used for (among others):

- Metadata (file name, collection name, font use, MIME type, and other attributes necessary to browse a collection).
- Saved application preferences.
- Information about the account holder such as name, email, licenses, and other basic user account information.

Data of members of an organisation with an Adobe ID are also not encrypted with the dedicated encryption key.

3.1.6 Projects

Projects are folders that can be shared between users and allow users to organise their assets.[221] More details on projects are available in Section 3.2.3.4. The Admin Console allows administrators to (see Figure 16):

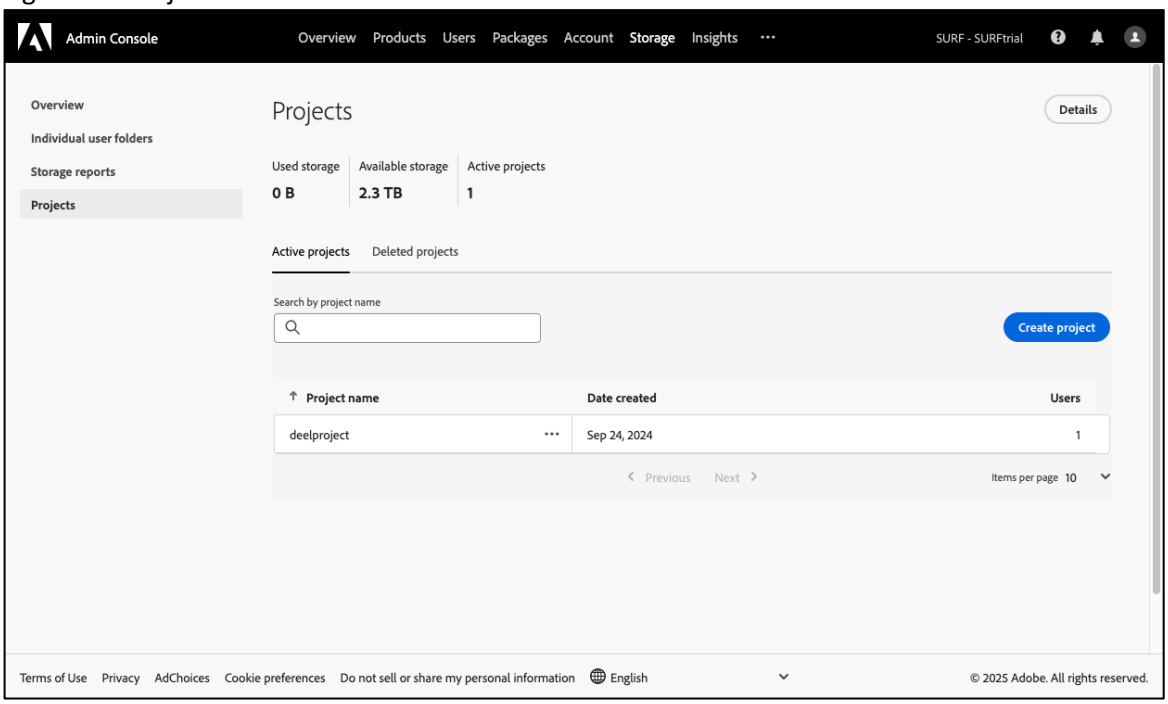
- View a list of existing projects.
- Create, rename and delete projects.
- Invite users to or remove users from a project (users can have edit or comment permissions).
- Set the default access level for a project (only invited users have access or the whole organisation can comment).
- Recover deleted projects or permanently delete them. The specific retention period for deleted projects is unclear. The documentation mentions that deleted projects can be restored *"at any time"*, although end-users are told projects are kept for 30 days when removing a project.[222] Adobe clarified that: *"Deleted Projects can be restored within 30 days from the date of deletion. The retention period for Projects is the same as for any other content or asset in ESM, where the content persists until Administrators either reassign them to another or completely delete them from our systems."*[223] Thirty days after testing, Privacy Company no longer observed deleted projects in the admin console. Given these answers, it is still unclear if projects are actually permanently deleted 30 days after removal by a user, or persist until an administrator deleted them.

[221] Manage projects, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/projects-in-business-storage.html.

[222] Manage projects, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/projects-in-business-storage.html.

[223] Email Adobe to SURF, 28 March 2025.

Figure 16: Projects overview in Admin Console

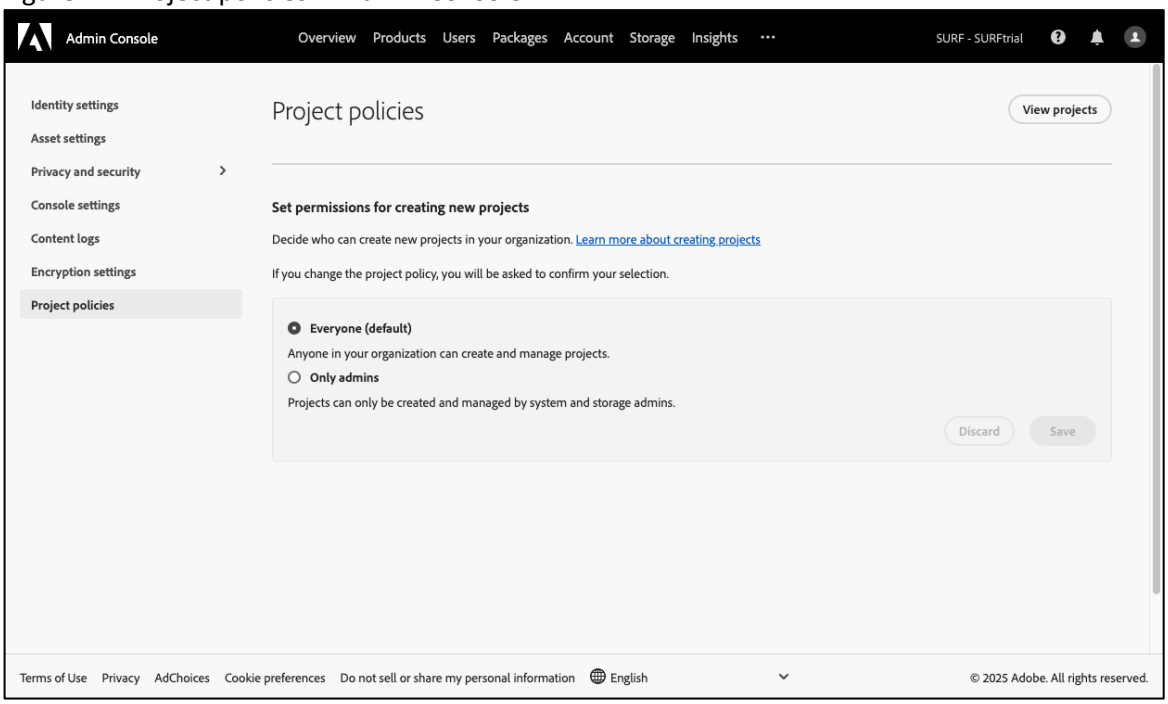


Depending on the project policy setting (*'Settings'* > *'Project policies'*), end-users are allowed to create projects or not (see Figure 17). If users are disallowed from creating projects, only administrators (system and storage admins) can create projects.

When an end-user creates a project, the fact that administrators can see the name of the created project is not mentioned directly, only in the documentation pages.[224] When administrators give other users (or themselves) access to a project, the original project creator is not notified of this change in access to the project.

[224] Creative Cloud projects overview, last updated: 30 December 2024, URL: https://helpx.adobe.com/sg/creative-cloud/help/projects-overview.html.

Figure 17: Project policies in Admin Console



3.1.7 Sharing restrictions

When it comes to sharing, administrators can manage sharing restrictions for assets (i.e. content) using the page *'Settings'* > *'Asset settings'* control in the Admin Console (see Figure 18). Administrators can turn off public link sharing and limit collaboration to the trusted domain, which means that students can only share content with other users within trusted organisations and external sharing would be completely disabled.[225] In total there are three sharing levels available:

- No restrictions (default setting).
- No public link sharing, but assets can still be shared with anyone outside of the organisation by email address.
- Sharing only to domain users, only allowing sharing with users on the authorized domains list.

The sharing restrictions apply to all Adobe Creative Cloud and Document Cloud applications, as listed in the documentation.[226] When sharing is only allowed with domain users, the list of domains includes the organisation's 'claimed', 'trusted' and 'authorized' domains. The claimed domains are the organisation's own domains. The trusted domains are the domains of directories that the organisation has trusted.[227] Authorized domains can be added through a separate tab on the Asset settings page.

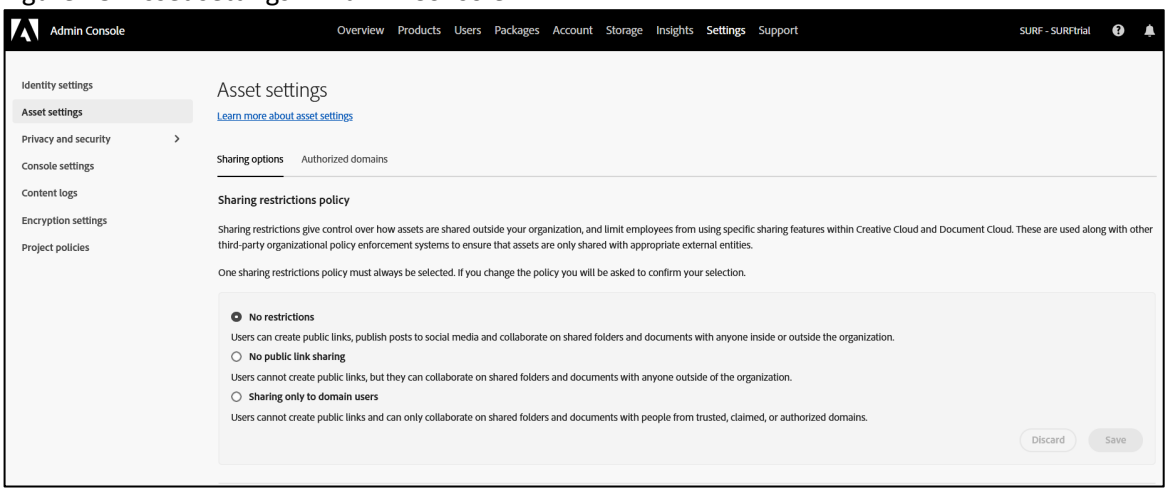
[225] Email Adobe to SURF 26 July 2024.

[226] Asset settings, last updated: 30 July 2024, URL: https://helpx.adobe.com/enterprise/using/asset-settings.html.

[227] Set up organization via directory trust, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/directory-trust.html.

On the same page in the Admin Console, it is also possible to disallow ‘access requests’. Access requests can be made by users when visiting a shared asset link they do not have access to. If a user makes an access request, all users with sharing permissions on the document will receive a notification and can choose to grant access to the document.[228]

Figure 18: Asset settings in Admin Console



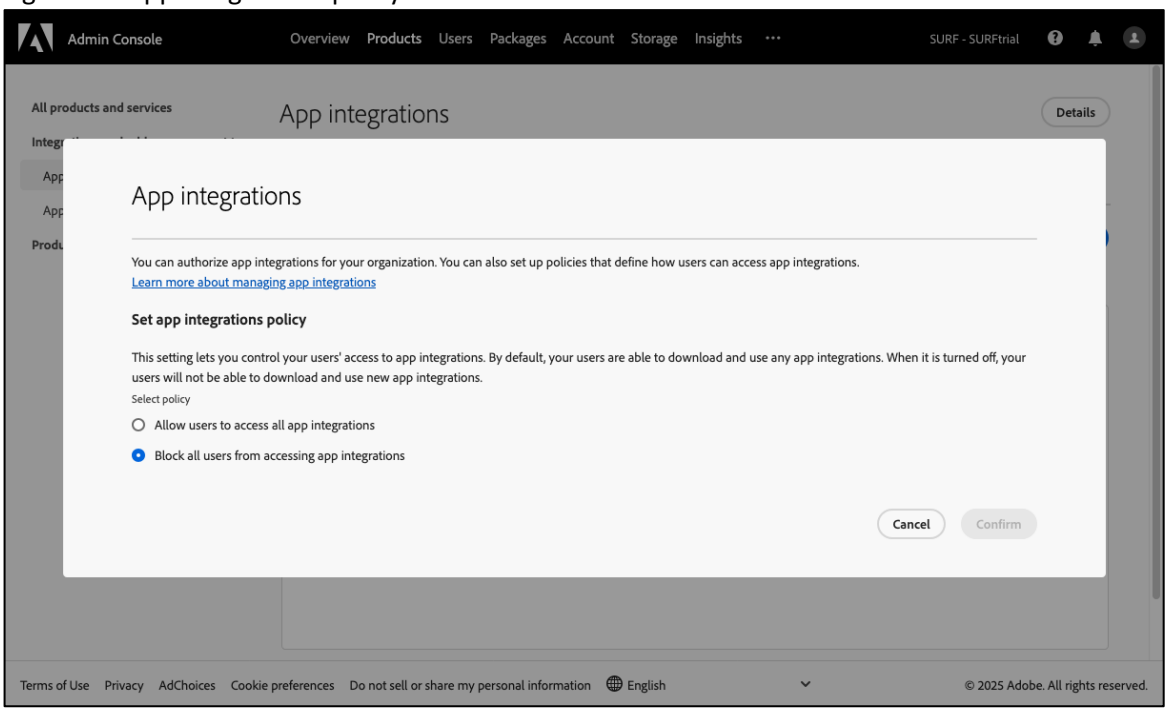
3.1.8 App integrations

App integrations allow third-party applications access to the Adobe APIs.[229] This makes it possible to read and write user information and Creative Cloud assets. Through the Admin Console, it is possible to block all users from accessing app integrations (see Figure 19). It is also possible to allow access to specific app integrations for all or specific users.

[228] Asset settings, last updated: 30 July 2024, URL: https://helpx.adobe.com/enterprise/using/asset-settings.html.

[229] Manage app integrations, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/manage-app-integrations.html.

Figure 19: App integrations policy in Admin Console



3.1.9 Add-ons policy

Add-ons are optional modules that extend the functionality of Adobe Express.[230] These modules can store and retrieve data, connect to external sources, import and export images and manipulate the image canvas. The add-ons are offered by Adobe and third-party developers. In case of add-ons by third-party developers, the Adobe privacy policy and terms of use are not applicable. The PSLT states that Adobe *"provide access to such third-party services as a convenience only."* [231]

Through the admin console, users can be blocked *"from downloading and installing add-ons"* (more precise: using add-ons, as Adobe Express is an online application accessed through the web browser). This setting is displayed in Figure 20. If this option is selected, users can only access three applications: OneDrive, Google Drive and Quick QR Code (see Figure 21). The first two applications are provided by Adobe. The last application seems to be provided by an individual employed by Adobe but falls outside of Adobe's privacy policy according to the description shown in Adobe Express.[232] Adobe has clarified that this is a native feature that falls under Adobe's policies, and that work is underway to clarify this in the

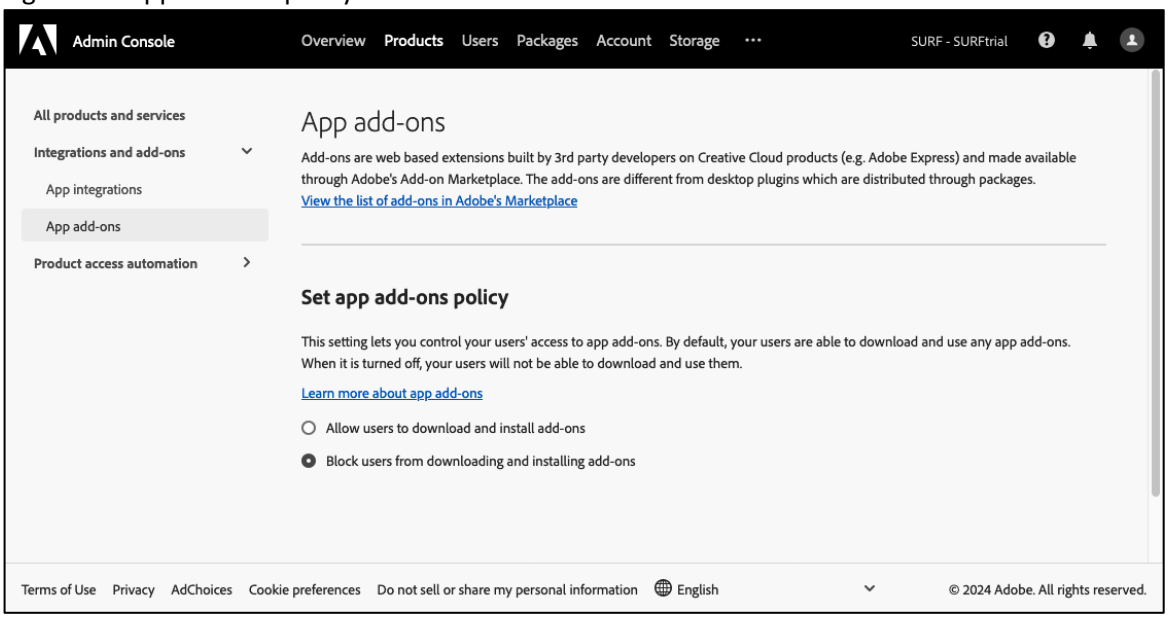
[230] Adobe Express Add-Ons Guides – Overview, last updated: 2 October 2024, URL: https://developer.adobe.com/express/add-ons/docs/guides/.

[231] Article 32.1, Adobe, PSLT – Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1), URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-CreativeCloudandDocumentCloudSubstance3D-WW-2023v1.pdf.

[232] See URL: https://new.express.adobe.com/add-ons?addOnId=wkmih82l8, last visited 4 February 2025.

interface of the product.[233] There is no option available to block all add-ons or to specify the specific add-ons to block or allow. Adobe intends to add more granular controls in the future.[234]

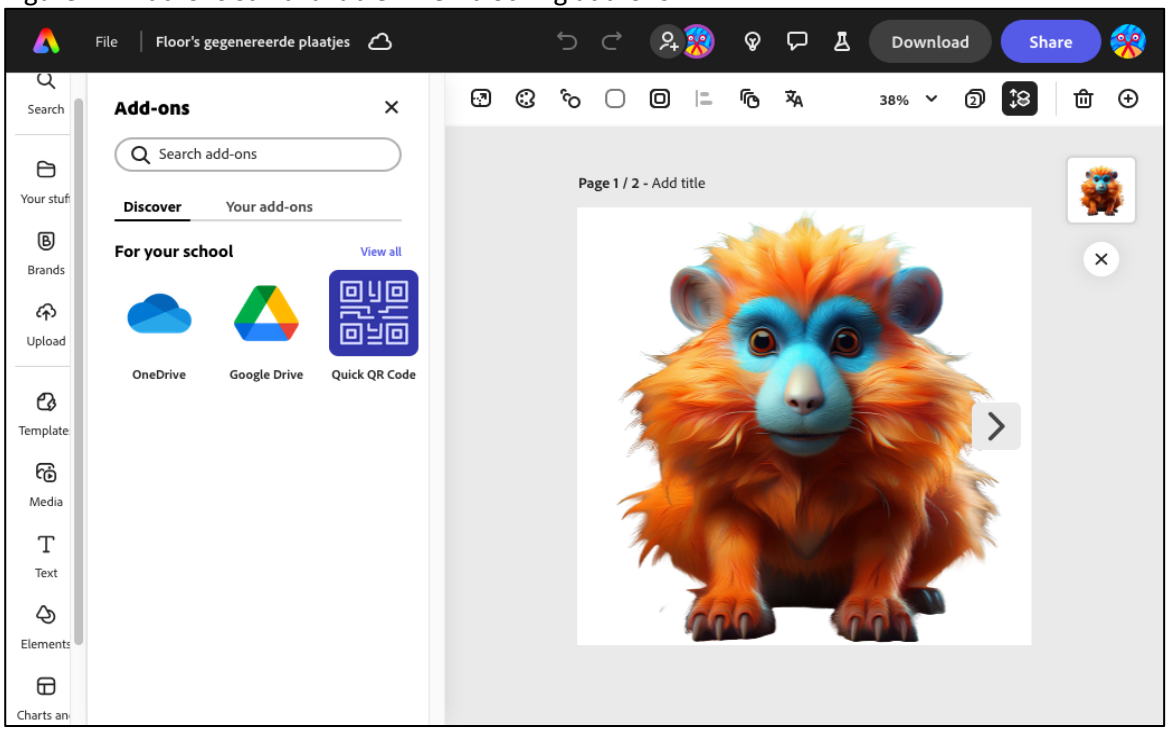
Figure 20: App add-ons policy in Admin Console



[233] Email Adobe to SURF, 14 February 2025.

[234] Email Adobe to SURF, 4 April 2025: *"Adobe introduced add-ons in 2023 to enhance the functionality of features in Express. To help organizations manage access, an add-on setting in the Admin Console allows admins to restrict usage within their organization. In 2024, responding to customer feedback, Adobe launched a set of default add-ons tailored for the K-12 experience, focusing on frequently used tools for education. Looking ahead, future K-12 add-on development will include more granular controls, enabling admins to disable default add-ons as needed."*

Figure 21: Add-ons still available when blocking add-ons



3.1.10 Custom font management

Administrators of enterprises can accept a 'custom fonts offer' in the Admin Console. After accepting this offer, administrators can upload custom fonts for use in the organisation. When adding a custom font, the administrator has to confirm the license of the font and acknowledge that the organisation holds a valid license to distribute the font. The administrator also has to *"give permission to Adobe, Inc. to share information pertinent to your font license with the publishing font foundry, such as company name and number of seats to which you have provisioned the fonts"*.[235]

End-users can only upload custom fonts to Adobe Express. This functionality is enabled by default. When uploading a custom font, the end-user is asked to acknowledge that they have *"all necessary rights and licenses to allow upload, storage, and access of that font in Creative Cloud"*. Administrators can disable this feature by disabling the 'User Font Upload' service in the product profile.[236]

3.1.11 Content logs

The Admin Console provides administrators with the option to export 'Content logs' (*'Settings'* > *'Content logs'*). These log files give detailed *"information on how end users are working with corporate assets"*.[237] They contain details for all users in directories owned by the organisation. Only assets on Enterprise Storage (see Section 3.1.5) are included in the logs and thus personal assets of users with an Adobe ID are not in the logs. The log files are offered as downloadable

[235] Upload and share custom fonts, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/custom-fonts.html.

[236] Upload and share custom fonts, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/custom-fonts.html.

[237] Content Logs, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/content-logs.html.

CSV files and log entries are available for 90 days, with an exported log file being available for 7 days. The log files contain entries on:

- Create, read, update, move and delete of assets.
- Sending, accepting and changing sharing on assets.
- Public link creating, reading and removing.
- Access requests and responses.
- Auto-added collaborators by accessing a public link.

Log entries consist of:

- Action (e.g., 'Read', 'Updated')
- Timestamp
- User (name, email)
- Item (path, file name, ID, create and update timestamps)
- IP address performing the action
- Collaborator details (name, email, role of the user that's being shared with)

Not all actions are logged: Adobe Lightroom, Behance and Stock are completely excluded.[238]

The logs also show asset access by internal Adobe services. These accesses can be recognised by a service account listed as user email in the logs. Adobe clarified these service accounts as follows:[239]

- **RenditionServiceSP**: a client of the rendition service used to generate and garbage collect renditions for assets in Adobe cloud storage (a derived, low-resolution representation of an asset).
- **AdobeIndexingService1**: a client of the indexing service used in conjunction with Adobe's universal search service (e.g., asset search).
- **Acp-cs-willie-sc**: a garbage collection service for asset, asset versions, and renditions for every update of an asset with version metadata, needed for the proper operations of user assets in Adobe cloud storage.
- **Xdnascanner_rapi2**: a client part of the Photo and VideoDNA service for scanning for potential registered child abuse material, supporting Trust and Service workflows in assets in Adobe cloud storage.

3.1.12 Audit logs

The Admin Console also provides an 'Audit log' to administrators (*'Insights'* > *'Logs'* > *'Audit log'*, see Figure 22). The audit log *"helps ensuring continued compliance, safeguarding against any inappropriate system access, and auditing suspicious behavior within your organization"*.[240] Events in the audit log are retained for 90 days and can be exported to a CSV file.

Adobe does not specify which actions are logged to the audit log. During testing, creation and deletion of a user, license assignments and user (admin) role assignments were logged.

---

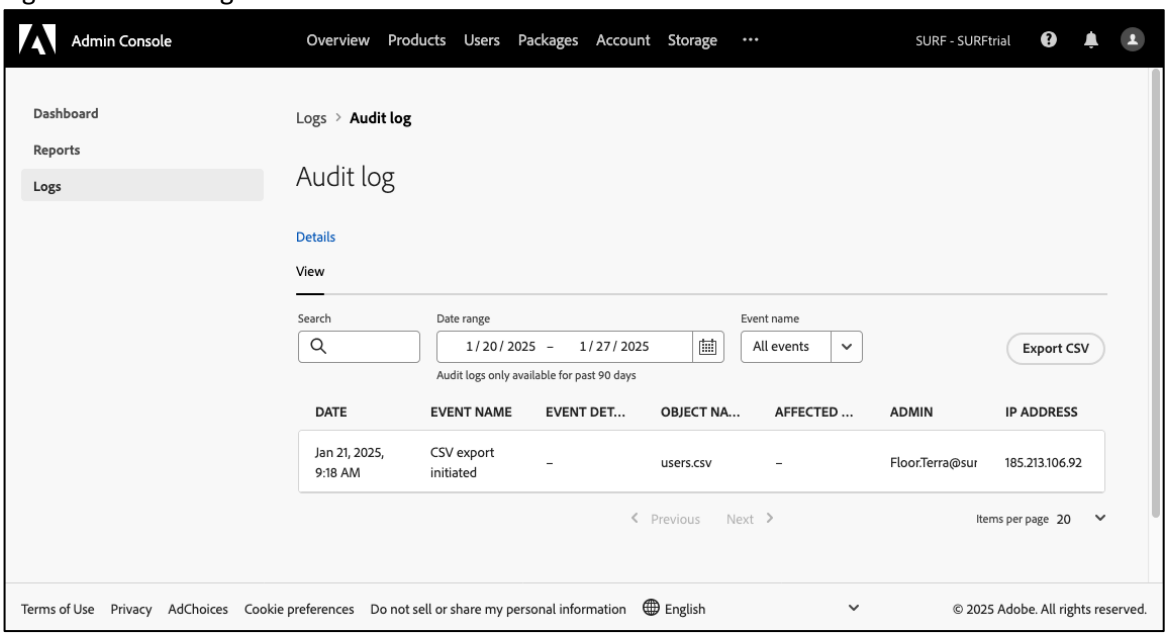
[238] Content Logs, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/content-logs.html. This document also mentions sharing actions are excluded for Adobe Express and InDesign, but Adobe clarified to SURF in an email on 28 March 2025 that this is no longer the case and that the HelpX article will be updated to reflect this.

[239] Email Adobe to SURF of 9 January 2025.

[240] Use audit log to track user assignments and events, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/audit-logs.html.

Organisational setting changes were only logged in some cases. E.g., disabling add-ons was logged but disabling sharing was not. Giving a user access to a project was not logged.

Figure 22: Audit log shown in Admin Console



3.2 Privacy Controls for end users

This section describes seven different privacy controls end-users can exercise:

1. Cookie and advertisement management
2. Account portal
3. Asset management and sharing
4. Redaction
5. Exports, metadata and content credentials
6. Integrations and add-ons
7. Desktop-specific features and preferences

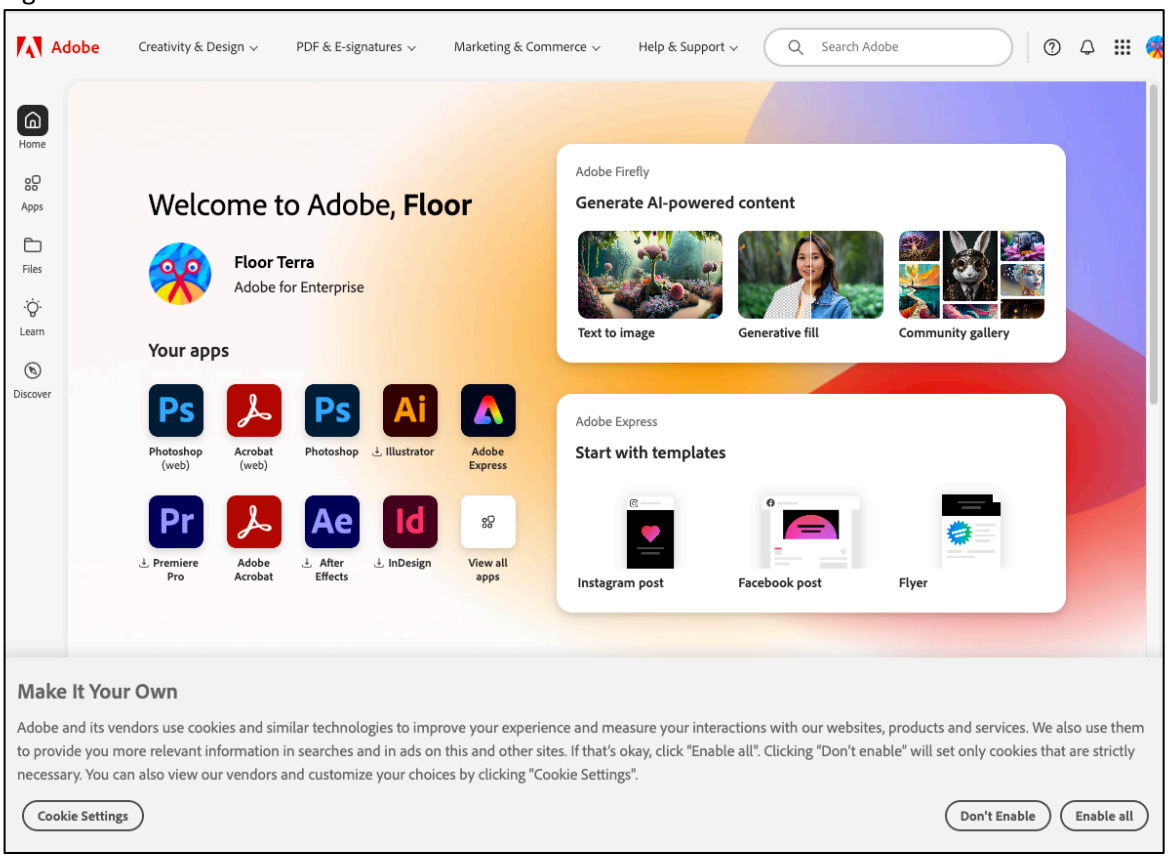
3.2.1 Cookie and advertisement management

3.2.1.1 Cookie consent

The Adobe websites show a *cookie consent banner* on first visit (see Figure 23). The cookie banner asks the user to enable cookies for the following purposes:

- Improve your experience
- Measure your interactions with our websites, products and services
- Providing more relevant information in searches on this and other sites
- Providing more relevant information in ads on this and other sites

Figure 23: Cookie consent banner on adobe.com



The banner allows customising the selection of cookies with the *'Cookie Settings'* button. It then presents a screen that allows the user a choice between the following purposes (see Figure 24):

- Operate the site and core services (always enabled)
- Measure performance
- Extend functionality
- Personalize advertising

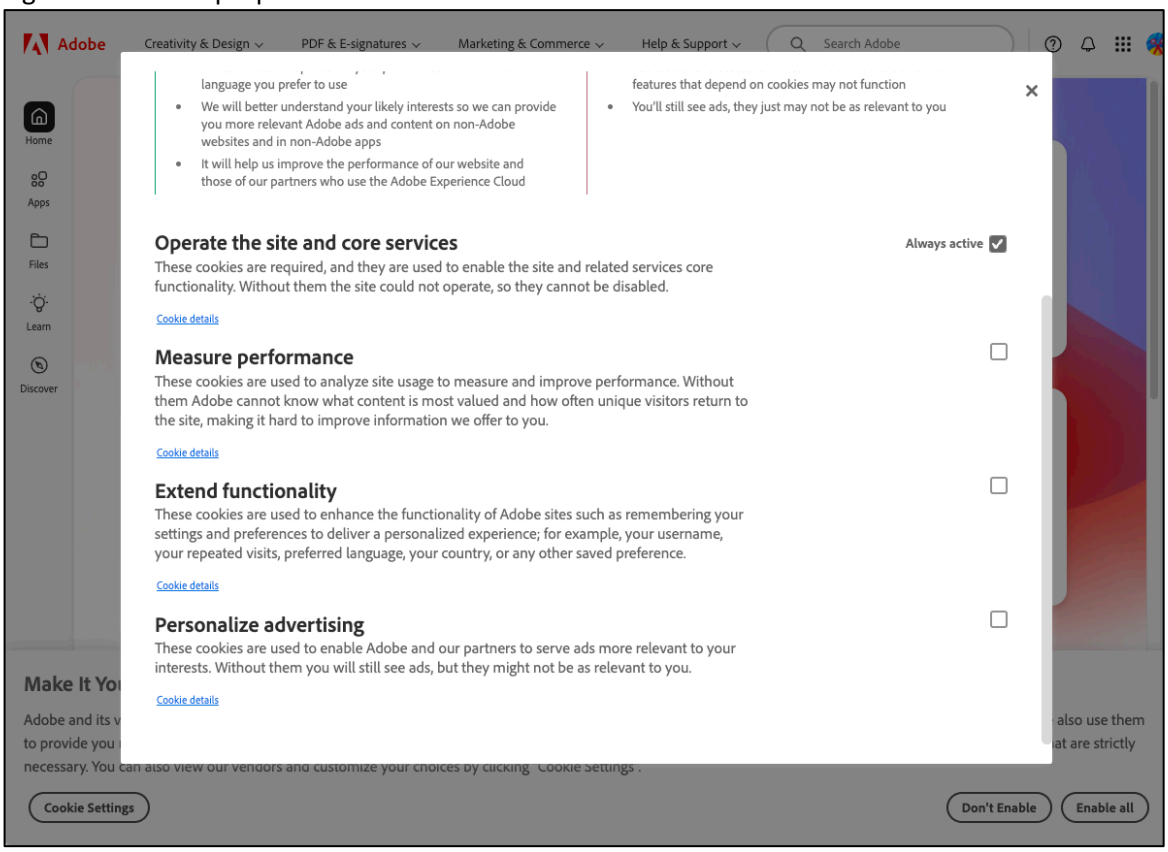
Under the *'Cookie details'* of each category, the popup lists the cookies with their name, host, duration, type and category. Under the category 'Operate the site and core services', cookies are listed for several domains that do not seem to be core services, including:

1. linkedin.com (third-party social networking site)
2. marketo.com (Adobe Experience Cloud marketing automation)
3. addtoany.com (third-party share buttons)
4. tradedoubler.com (third-party affiliate marketing)
5. tribalfusion.com (third-party advertisement network)

Update after completion of Part A

Adobe has resolved the misclassified cookies and classified the cookies as advertising cookies. Furthermore, educational users can no longer opt-in to personalised advertising. See Section 2.3.3 for details. These updates have been taken into account in parts B-D of this DPIA.

Figure 24: Cookie purposes selection screen on adobe.com



Once the user has made a choice, the place the cookie consent screen can be opened again depends on the application: for Adobe Photoshop (web) the screen is readily available using a '*Cookies*' button at the bottom of the screen, for the other applications the profile or help button offers a menu with a *'Legal Notices'* button. This menu lists a *'Cookie Preferences'* option that opens the consent screen (see Figure 25 and Figure 26 for these options in Adobe Acrobat (web)).

Figure 25: Help menu with *'Legal notices'* button in Adobe Acrobat (web)

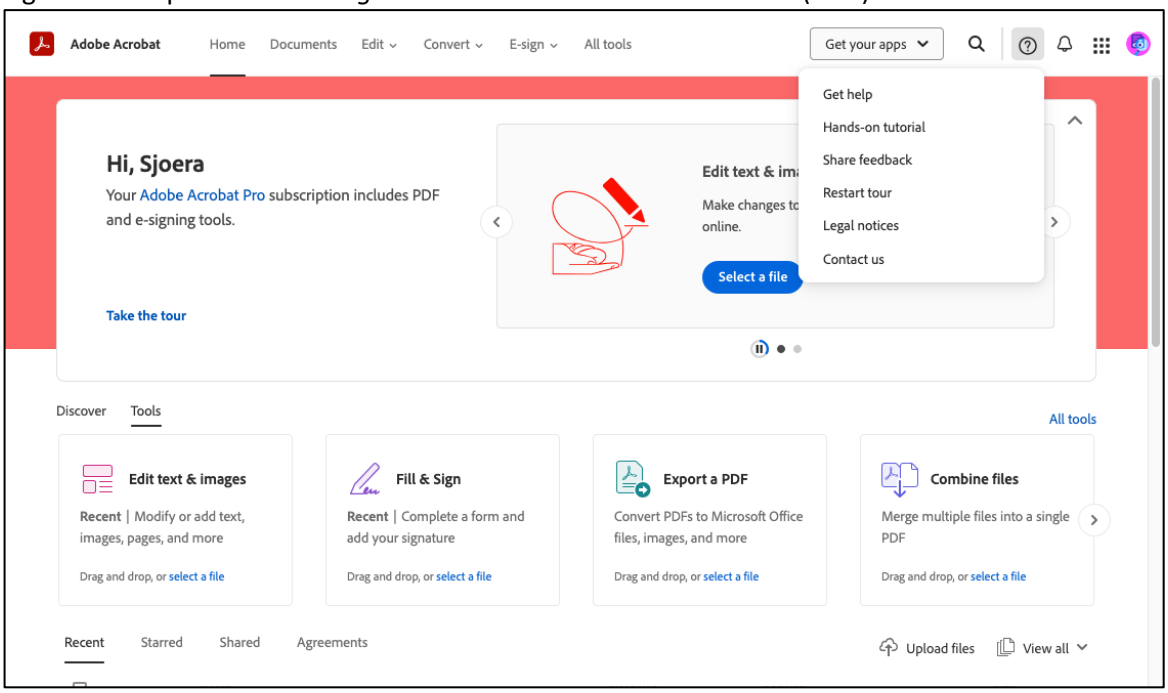
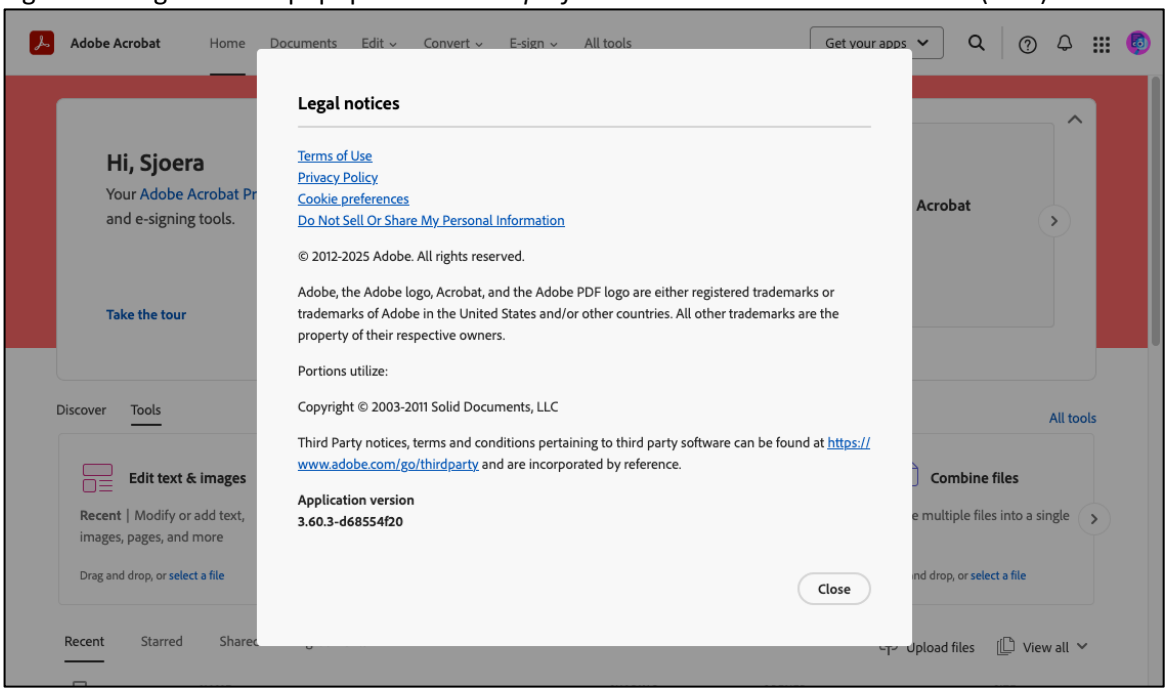


Figure 26: Legal notices popup with *'Cookie preferences'* button in Adobe Acrobat (web)



3.2.1.2 AdChoices

In addition to the cookie consent screen, Adobe offers the user additional opt-out choices on the Adobe Privacy Choices webpage.[241] A link to this webpage is present in some products, but not all. Adobe Photoshop (web) prominently displays an *'AdChoices'* link at the bottom of the screen

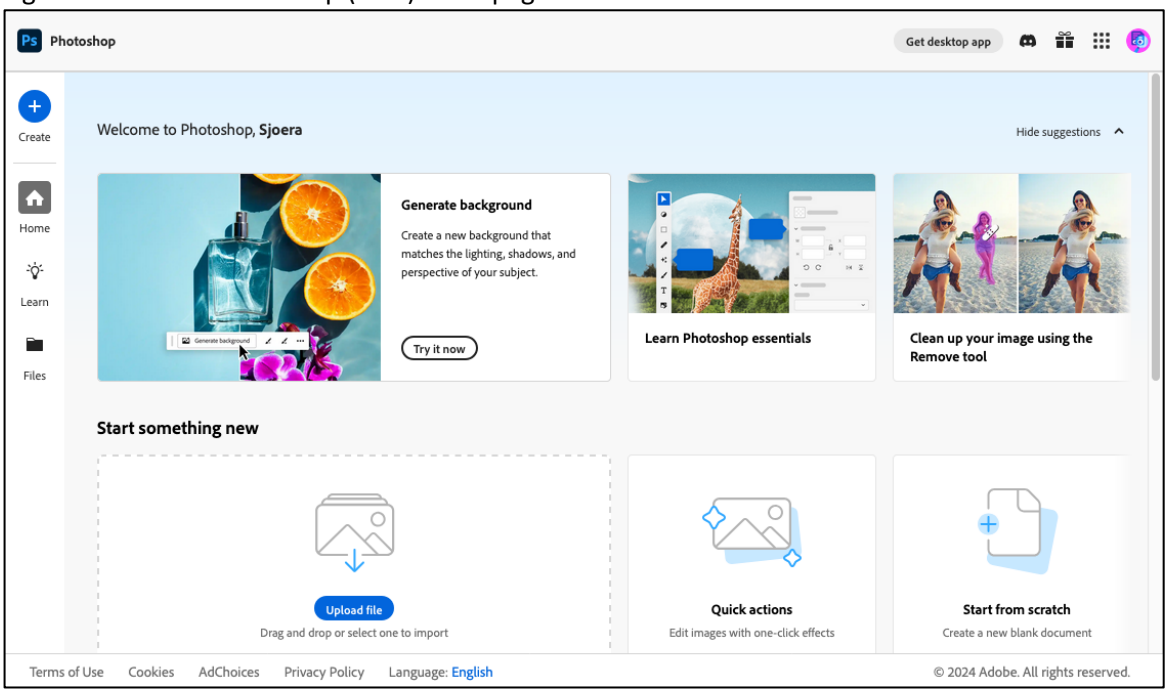
[241] Adobe Privacy Choices, last updated: 18 June 2024, URL: https://www.adobe.com/privacy/opt-out.html.

(see Figure 27) and Adobe Express shows the same link in the *'Legal notices'* submenu. The Creative Cloud homepage and Adobe Acrobat (web) do not show this link.

Adobe clarified that AdChoices work in addition to the Adobe cookie banner:[242]

> *"the Adobe cookie consent banner manages the cookies set in our domains and web-based apps, while AdChoices allows users to make choices across all sites where Adobe Experience Cloud solutions run, operated by Adobe and any of our customers. The presence of the AdChoices link in Photoshop web [..] is an incorrect implementation that will be removed in an upcoming release."*

Figure 27: Adobe Photoshop (web) homepage with *'AdChoices'* link at the bottom

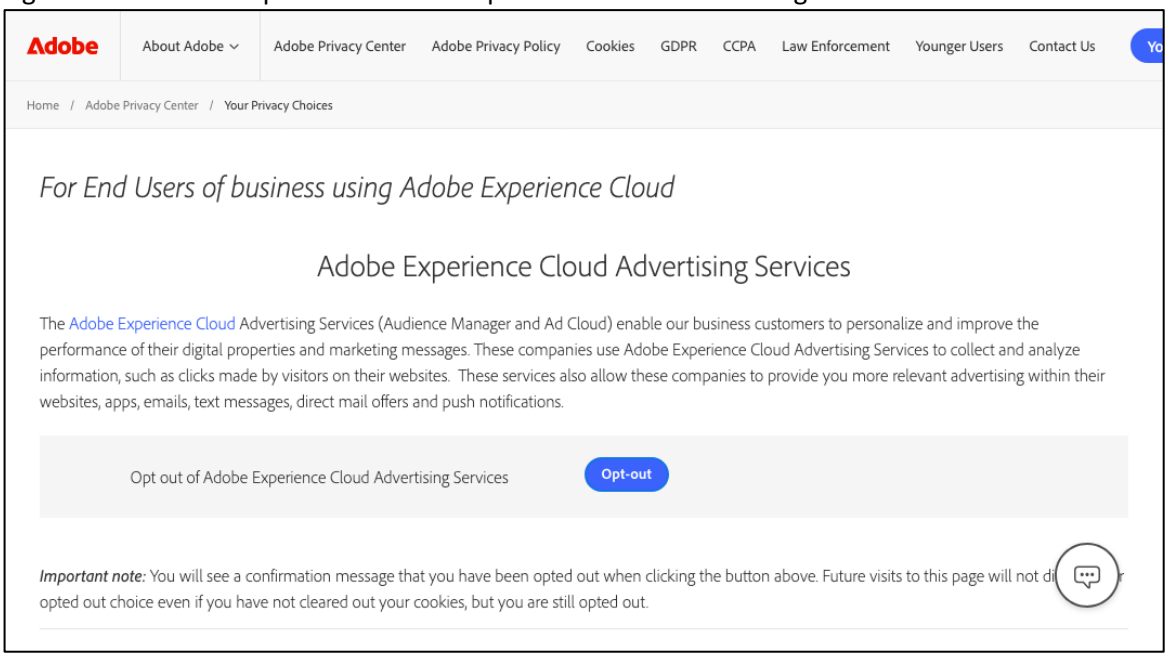


The Privacy Choices webpage shows the user a button to opt-out of 'Adobe Experience Cloud Advertising Services' (see Figure 28). In addition to this, it suggests the user to opt-out of interest-based ads by:

- Opting out at the following third-party sites:
  - Australian Digital Advertising Alliance (ADAA)
  - Digital Advertising Alliance (DAA)
  - European Interactive Digital Advertising Alliance (EDAA)
  - Network Advertising Initiative (NAI)
- Limiting ad tracking on your mobile device
- Downloading the Digital Advertising Alliance's AppChoices app

[242] Email Adobe to SURF, 4 April 2025.

Figure 28: Button to opt-out of Adobe Experience Cloud Advertising Services



Next to the Privacy Choices webpage, Adobe also has a webpage with opt-out choices for privacy regulations specific to certain states of the United States.[243] As these regulations are not applicable in Europe, they were not further considered.

3.2.2 Account portal

The Adobe account portal is available at https://account.adobe.com. This portal offers several pages with privacy-related settings.

3.2.2.1 Data and privacy settings

The data and privacy settings page allows users with a personal account to opt-out of content analysis for product improvement (see Figure 29). Users with a business or educational account are *"automatically opted out of content analysis for product improvement"*, as also explained on the page itself.[244] For personal accounts, there are also settings available to share 'Desktop app usage' (also known as telemetry). For business profiles (including Adobe IDs with business licenses assigned), this setting is not available as *"For these users, Adobe does not receive desktop app usage data"*.[245]

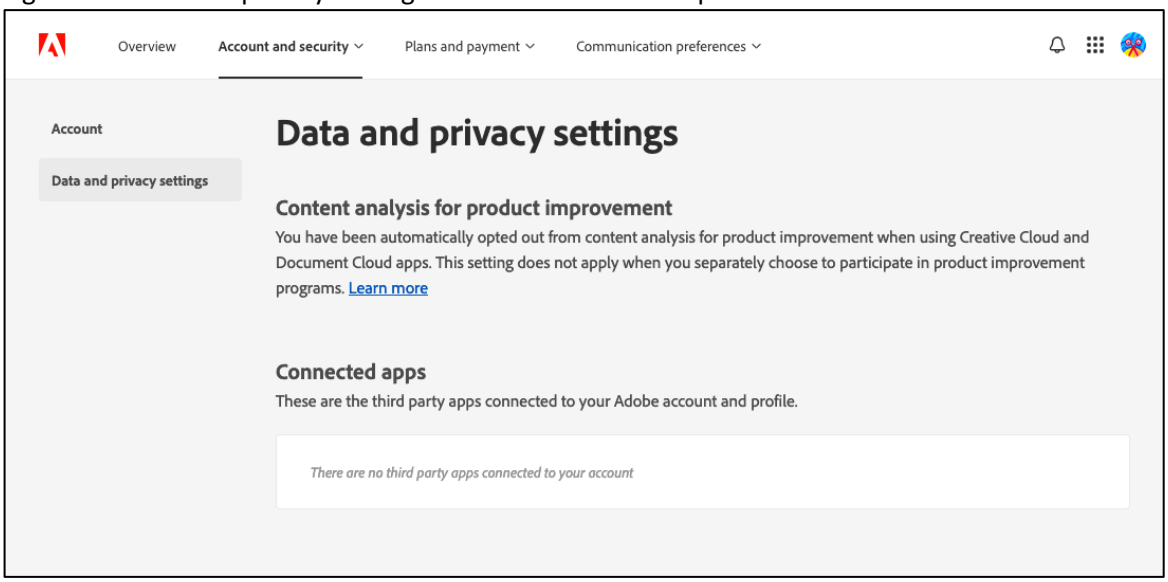
The page also shows 'connected apps' and allows to revoke access for these applications.

[243] Additional US State Privacy Rights, last updated 20 April 2023, URL: https://www.adobe.com/privacy/us-rights.html.

[244] Content Analysis FAQ, last updated 30 July 2024, URL: https://helpx.adobe.com/manage-account/using/machine-learning-faq.html.

[245] Usage Data FAQ: Creative Cloud and Document Cloud Apps, last updated 18 June 2024, URL: https://www.adobe.com/privacy/app-usage-info-faq.html

Figure 29: Data and privacy settings in the Adobe Account portal



3.2.2.2 Marketing newsletters

Users can subscribe to newsletters in the Adobe Account panel (see Figure 30). The content of these newsletters ranges from product and security updates to event announcements and creative inspiration. In their Adobe & Student Privacy document, Adobe mentions that they do *"not market to student users with Enterprise or Federated IDs"*.[246] In response to questions, Adobe indicated that *"HED users can also opt in to marketing, whereas a K12 end user is restricted by default from being able to opt in to marketing"*.[247]

Adobe further explained that it already *"has in a place a system that identifies email addresses associated to K12 student users and records them as "opted out" for email marketing communications. As a result, K12 student users are blocked from all non-operational messages sent by Adobe systems."*[248]

Nevertheless, in all cases it was possible to subscribe to newsletters through the account settings, even when using a Federated ID that only has an Adobe Express K12 license assigned. After being subscribed to all newsletters for several weeks, the test user only received one security bulletin and no other newsletter emails. This suggests that, although users can subscribe, they may still be filtered out of receiving most newsletters and supports Adobe's statement that *"Even if they were to attempt to opt in to marketing emails, Adobe systems will change their opt in to an opt out upon identifying them as a primary or secondary school student user."*[249] This filtering is based on the school type and user role determined as discussed in Section 3.1.1.

For one test user that signed up for Behance (out of scope for this DPIA) with a Federated ID, a marketing email was received on 3 February 2025 (see Figure 31), even with all newsletter options disabled (see Figure 32).

[246] Adobe & Student Privacy, last updated 21 July 2021, URL: https://www.adobe.com/privacy/student-policy.html.

[247] Adobe DSAR Response from 30 October 2024, p. 12.

[248] September 2025 Response to SURF Concerning Technical Mitigations (4 Oct 2025).

[249] Email Adobe 13 December 2024.

Figure 30: Newsletter preferences in the Adobe Account portal

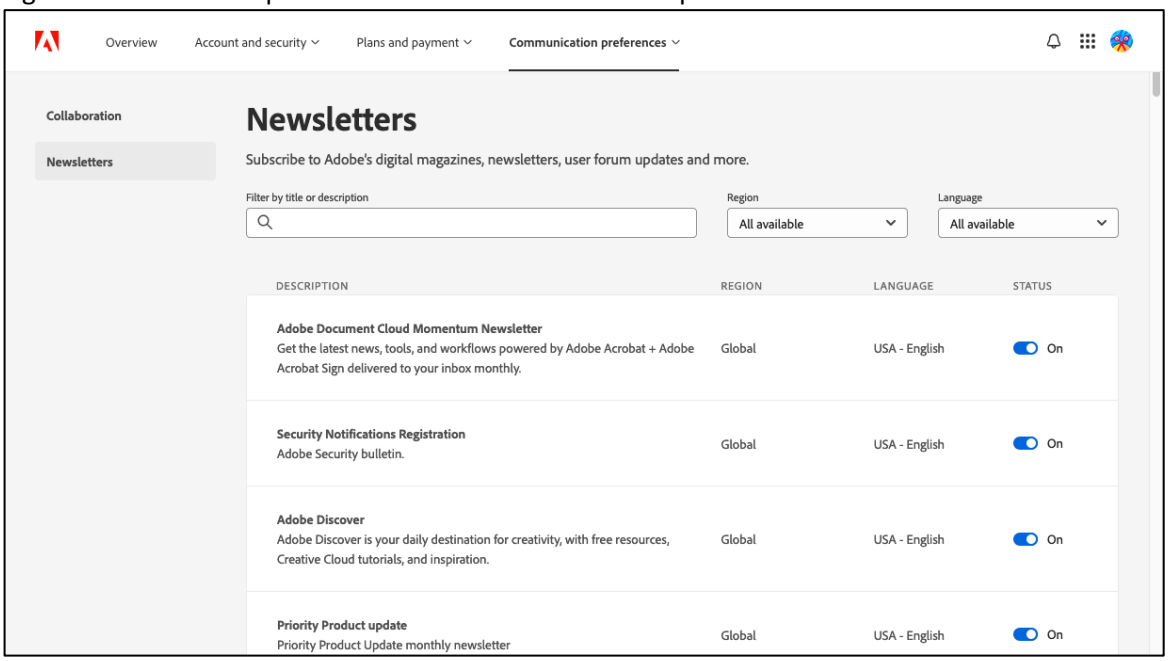


Figure 31: Behance marketing email as sent to test user

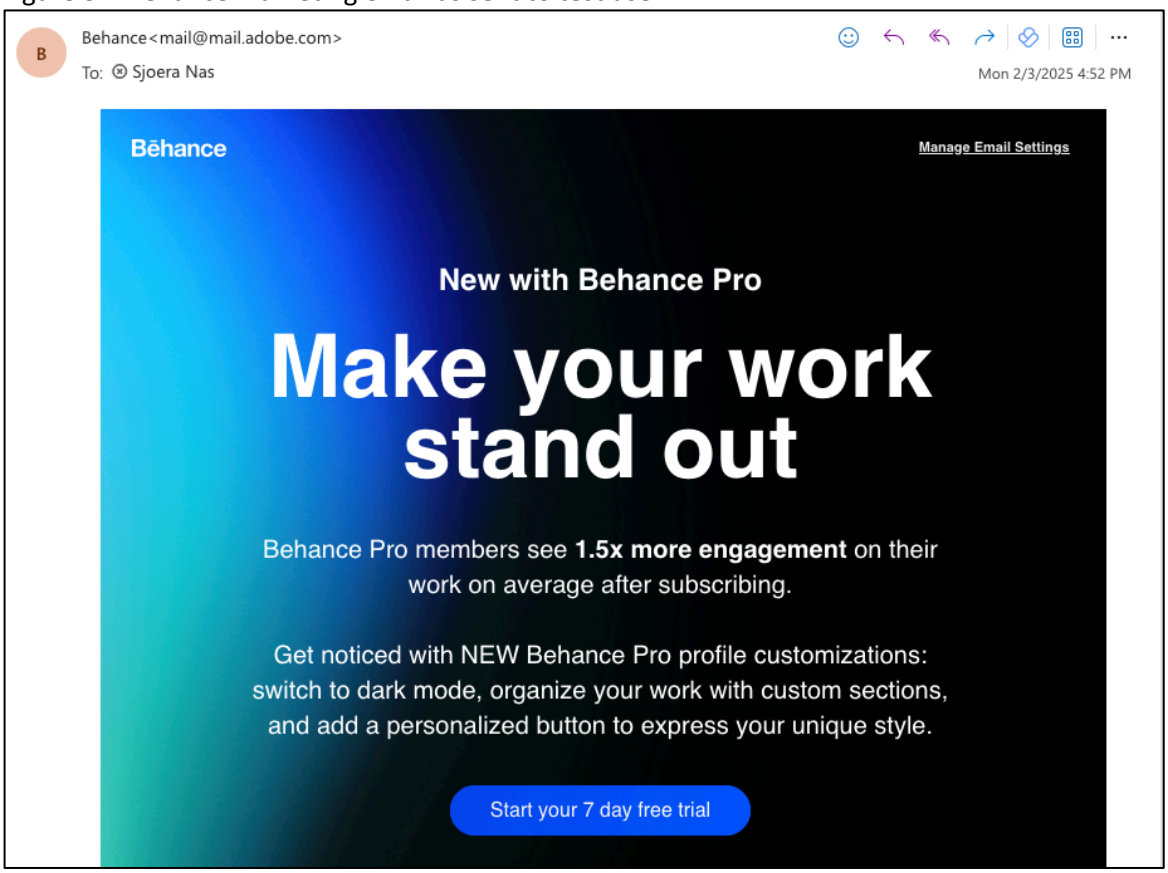
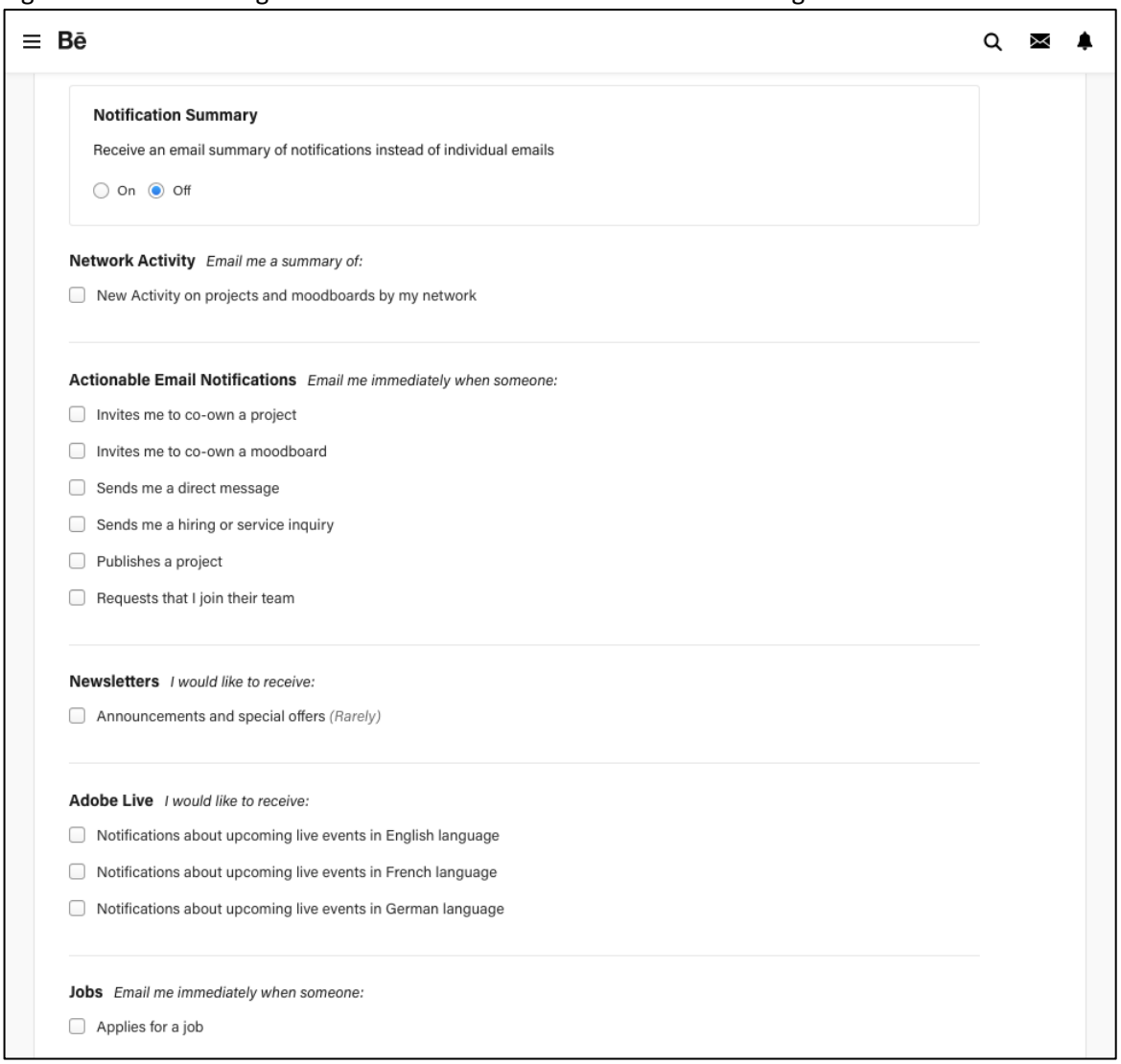


Figure 32: Email settings for the user that received Behance marketing email



Update after completion of Part A

A bug related to newsletter subscriptions was resolved in June 2025. This update has been taken into account in parts B-D of this DPIA.

3.2.3 Asset management and sharing

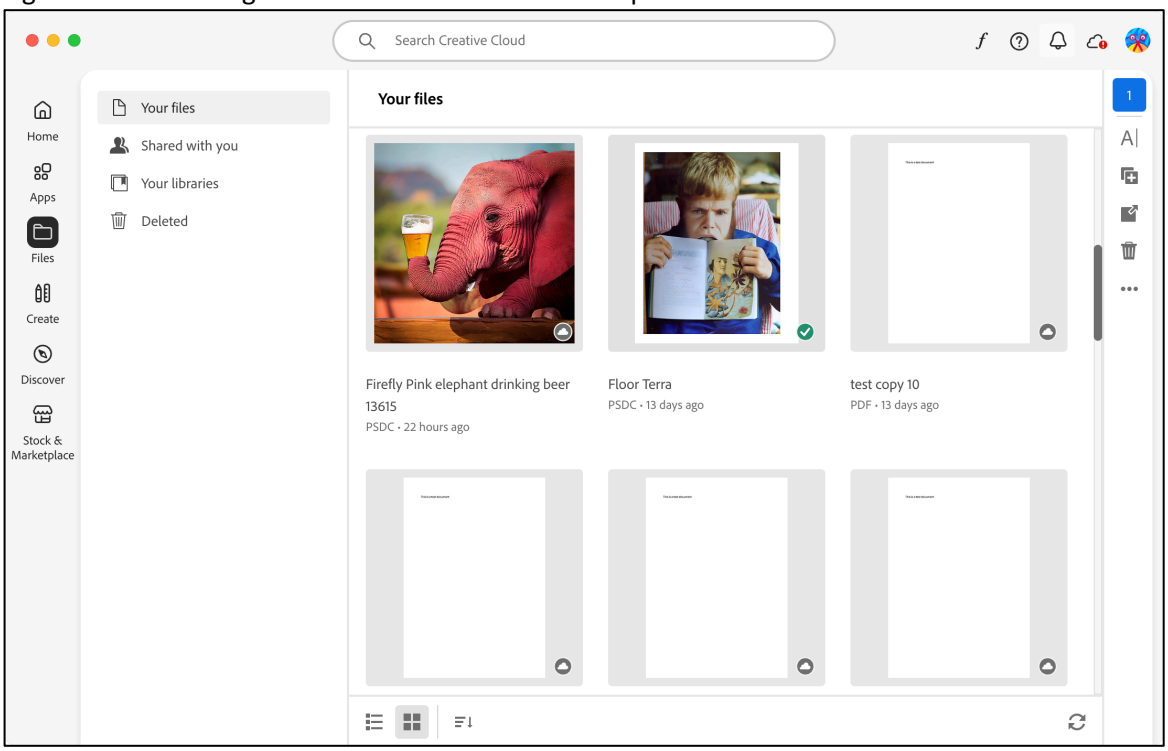
User assets (documents, files, images) can be stored locally, on the computer of the user, or in Adobe Cloud Storage. When using any of the online tools (Adobe Express, Photoshop web or Acrobat web), documents are always stored in Adobe Cloud Storage. This section discusses how users can manage and share their cloud assets.

3.2.3.1 Files and folders

Users can manage their files through the Creative Cloud web portal and the Creative Cloud desktop application. Both offer a view of the user's documents, including any Document Cloud

(Acrobat) documents, and allow moving, renaming and deleting documents (see Figure 33). Deleted documents are moved to a separate tab, where they are kept for 30 days and can be permanently deleted.[250]

Figure 33: File management in Creative Cloud desktop



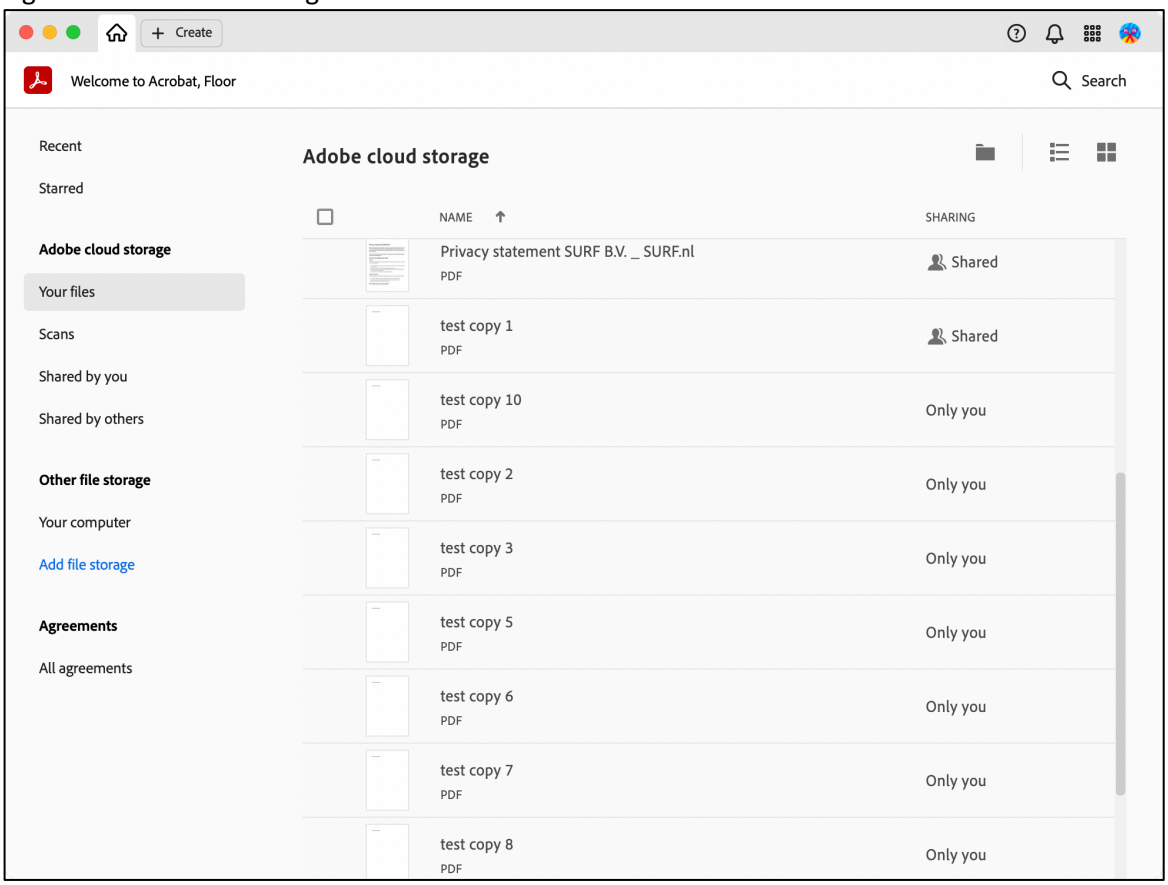
Files can be added by creating new files, uploading existing files from the local computer or duplicating existing files. Folders can be created to group files into a folder.

The welcome dialogs of both desktop applications (Acrobat and Photoshop) also show the cloud files in a similar list (see Figure 34). There, users can choose to open a cloud document but also have the option to open a document from their local computer. When saving a document, this is done on the local computer by default, but the user can choose to store to the cloud.

If a user opens a file from the local computer in one of the web applications (Acrobat or Photoshop), the file will be automatically uploaded and stored to Adobe Cloud Storage, without further warning (irrespective of whether users use an Adobe, Enterprise of Federated ID).

[250] Delete files permanently from cloud storage, last updated: 13 December 2024, URL: https://helpx.adobe.com/creative-cloud/help/delete-files-permanently.html.

Figure 34: Welcome dialog of Adobe Acrobat



Cloud documents are automatically saved. This means that when the user works in one of the web applications (Acrobat web, Photoshop web or Adobe Express) or when the user opens a document from the cloud in one of the desktop applications (Acrobat or Photoshop), any changes the user makes are automatically stored in the cloud.

There is no bulk transfer tool available to download all files of a user at once. If users want to download their data, for instance to migrate to another product or account, their options are[251]:

- Download files one by one in the Creative Cloud web application.
- Download a maximum of 10 files at a time in the Creative Cloud desktop application.
- Manually share files with another Adobe account and then store a copy of those files in the other Adobe account (see the next section).
- Use the Student File Transfer service to move files to another Adobe account (see Section 3.2.3.7).

Adobe Express files cannot be downloaded as they are online-only files.

[251] Transfer files across accounts or profiles, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/kb/transfer-assets.html.

3.2.3.2 Creative Cloud sharing

Users can share Creative Cloud assets (Photoshop or Adobe Express files) with other users within or outside of the organisation, depending on the organisation's sharing restrictions (see 3.1.7). Sharing an asset can be done through the Creative Cloud (web or desktop), Photoshop (web or desktop) or Adobe Express (web) applications.[252] By default, the following sharing options are available:

- Share with:
  - Individual users
  - Everyone in the organisation
  - Anyone with the sharing link (public sharing)
- Allowing:
  - Viewing only
  - Commenting (default when sharing with organisation or anyone)
  - Editing (always allowed when sharing with individual users)
  - Saving a copy (default off, only for Photoshop)

Sharing generates a link that can be shared with other users, giving them access to the document (based on the configured sharing level). When sharing with individual users, a message can be sent to the user, and the document shows up in the Creative Cloud application under *'Shared with you'*. Sharing settings can be reverted to *'unshare'* a document, making It no longer available to other users.[253]

During testing, Privacy Company observed some inconsistencies in the sharing processes:

- Allowing editing when sharing with the whole organisation or anyone is only available in Photoshop Web and Adobe Express (not in the desktop apps or Creative Cloud). If a user subsequently tries to revert these settings through the Creative Cloud application, the new sharing level does not persist, and the document keeps being shared. From that point, the user is also unable to revert sharing in the web applications, essentially meaning the document will be shared until it is deleted.[254]
- Administrators can always access a user's Creative Cloud files, even when the file is not explicitly shared with them, as long as they know the sharing link. The administrator can obtain the sharing links by interpreting the administrative content logs. This is by design, see Section 3.1.5.2 for a discussion on this matter.
- In Photoshop, users of the organisation were unable to comment when given this permission, but users outside of the organisation could comment.

Users cannot easily see which Creative Cloud files they have shared: the Creative Cloud web application does contain a *'Shared with'* column in its list view, but that only contains information (the number of contributors) if the file has been shared with individual contributors.

---

[252] Share a file or folder publicly, last updated: 6 October 2023, URL: https://helpx.adobe.com/creative-cloud/help/share.html.

[253] Collaboration FAQ, last updated: 6 October 2023, URL: https://helpx.adobe.com/creative-cloud/help/collaboration-faq.html.

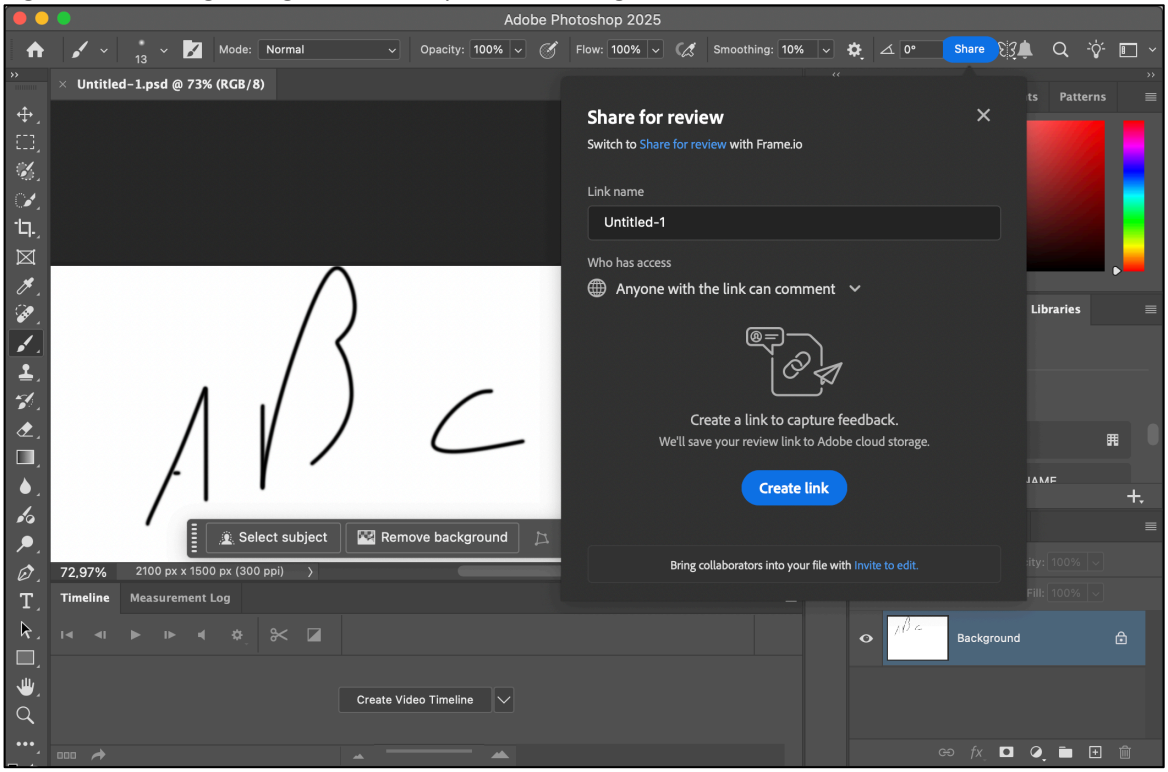
[254] Adobe has confirmed in an email to SURF on 28 March 2025 that *"This is a known issue in the Creative Cloud application. Adobe will be rolling out a fix to address this bug."*

If a file was shared with the whole organisation or anyone (or if it is a Document Cloud file), the column is empty. Adobe has confirmed they are working on improvements in this area.[255]

The Photoshop desktop application also allows creating *'Review links'*. These links allow sharing a read-only view of a document at a specific point in time, optionally protected with a password.[256] Optionally, users visiting the review link can be allowed to comment on the file. The review links are listed in the Creative Cloud web application and can be removed.

When sharing a locally stored file, the file is uploaded to Creative Cloud when the user shares the file. Users are reminded of this in the dialog when sharing the file (see Figure 35). If the file is subsequently unshared, the file will stay in Adobe Cloud Storage until it is manually removed by the user.

Figure 35: Sharing dialog in Photoshop when sharing a local file



3.2.3.3 Document Cloud sharing

For Document Cloud files (Adobe Acrobat), the sharing process is somewhat similar to the process for Creative Cloud files and also take the organisation's sharing restrictions into account. Sharing can be done through the Acrobat portal, web application or desktop application. Although the Document Cloud files are also displayed in the Creative Cloud portal, it is not possible to share from this portal.

[255] Email Adobe to SURF, 28 March 2025: *"We are aware of this, and investigations are underway to incorporate the capability to show when the document is shared in all cases in the referred list view. "*

[256] Share your documents for review, last updated: 10 May 2024, URL: https://helpx.adobe.com/photoshop/using/share-for-feedback.html.

The following sharing settings are available:

- Share with:
  - Individual users
  - Everyone in the organisation
  - Anyone with the sharing link (public sharing)
- Allowing:
  - Viewing only
  - Commenting (default)

Sharing generates a sharing link which can be shared to collaborators. It is also possible to send a notification with a specific message to the collaborator or send an email (Acrobat desktop). An overview of shared documents is available in the *'Shared by you'* tab in the Acrobat portal, allowing easy *'unsharing'* of files. Administrators cannot access shared documents unless they have access in accordance with the sharing level set for the document. When sharing a local document, the document is automatically uploaded to Adobe Cloud Storage. This is mentioned in the sharing dialog.

3.2.3.4 Projects

Users can create *Projects* that can be used to share assets (images, documents, other files) with other users, if the administrator allows this (see Section 3.1.6).[257] Invited users can get access *edit* or *comment* permissions. Depending on the organisation's sharing settings (see Section 3.1.7), external users can be invited. It is also possible to give *comment* access to all users in the organisation. All users with *edit* permissions can delete a project from the organisation. These deleted projects can be recovered for 30 days by any user that previously had *edit* permissions or administrators.

Projects are not well supported by the desktop applications, e.g.: Creative Cloud desktop does not list projects and Photoshop or Acrobat cannot directly open files from projects. In some cases, it is possible to open and edit a file in a project by choosing 'Open in desktop app', but in those cases not all features are available in the desktop apps (e.g., sharing gives an error).

3.2.3.5 Libraries

Users can also create *Libraries*, which are used to gather design elements for projects, clients or teams (e.g., fonts, colours, templates and other assets).[258] Libraries are also available in the Creative Cloud desktop applications.

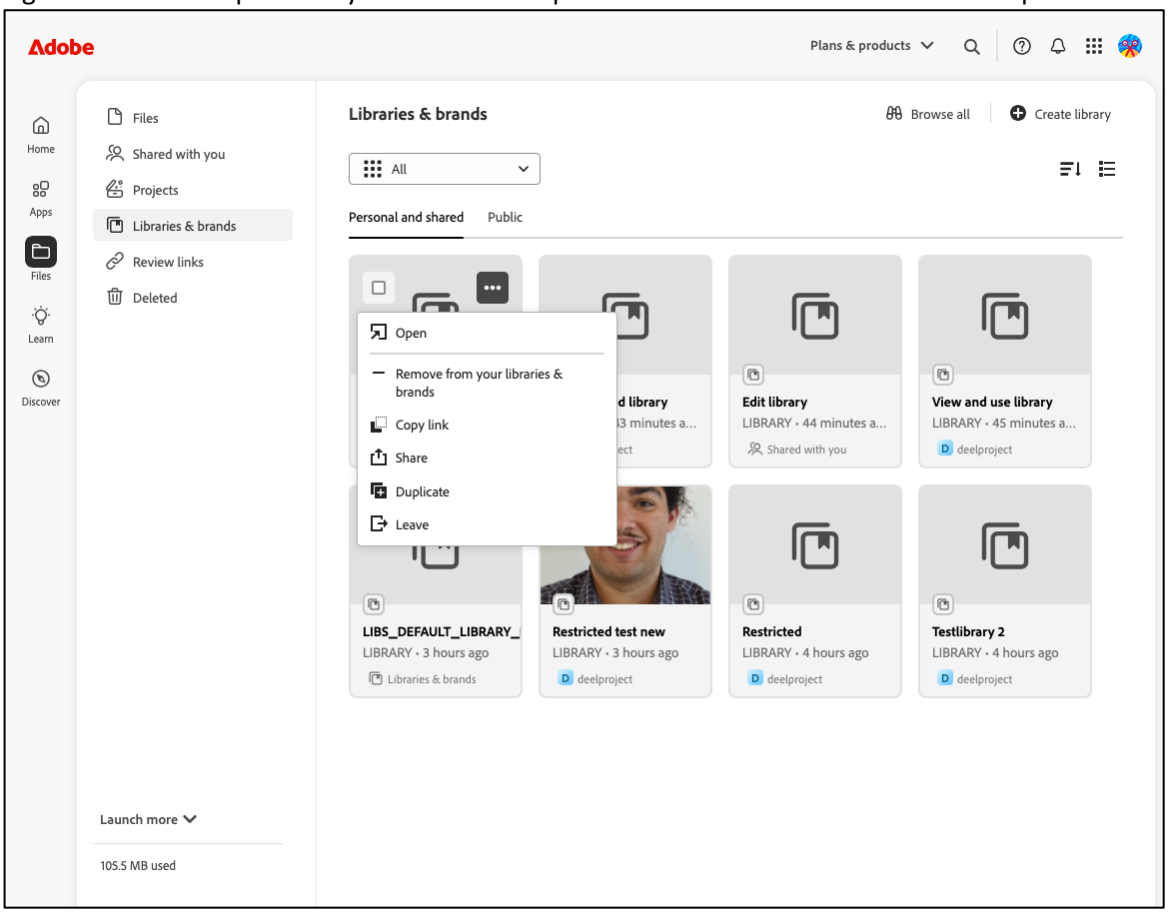
Libraries can be stored in the user's personal storage or in a project. When stored in the user's personal storage, they can be shared with other users, in a similar way as projects or folders. The access level can be *view* or *edit*. When stored in a project, all project members have access to the library by default. The access level can be *restricted* (*view and use* in Creative Cloud desktop) or *unrestricted* (*edit* in Creative Cloud desktop). With *restricted* access, other project members can only view and use the library contents but not change them.

[257] Creative Cloud projects overview, last updated 30 December 2024, URL: https://helpx.adobe.com/sg/creative-cloud/help/projects-overview.html.

[258] Creative Cloud Libraries, last updated 27 December 2024, URL: https://helpx.adobe.com/sg/creative-cloud/help/libraries.html.

Creating a project library with *restricted* permissions leads to problems when the creating user chooses to *'Leave'* the library (which is the only option the Creative Cloud web application offers for such libraries, as the *'Delete'* option is only available in the desktop interface, see Figure 36). In these cases, their own permissions are removed, and they are no longer able to remove the library or files in that library. This can lead to a situation where none of the users in the organisation is able to remove the files from the library and the only option is to delete the whole project containing the library.

Figure 36: Libraries panel only shows *'Leave'* option for restricted libraries in the web portal



Update after completion of Part A

Adobe recognizes that the user experience is different between desktop and web and will change the web experience to match the experience on Adobe Creative Cloud Desktop.[259]

3.2.3.6 Document versioning

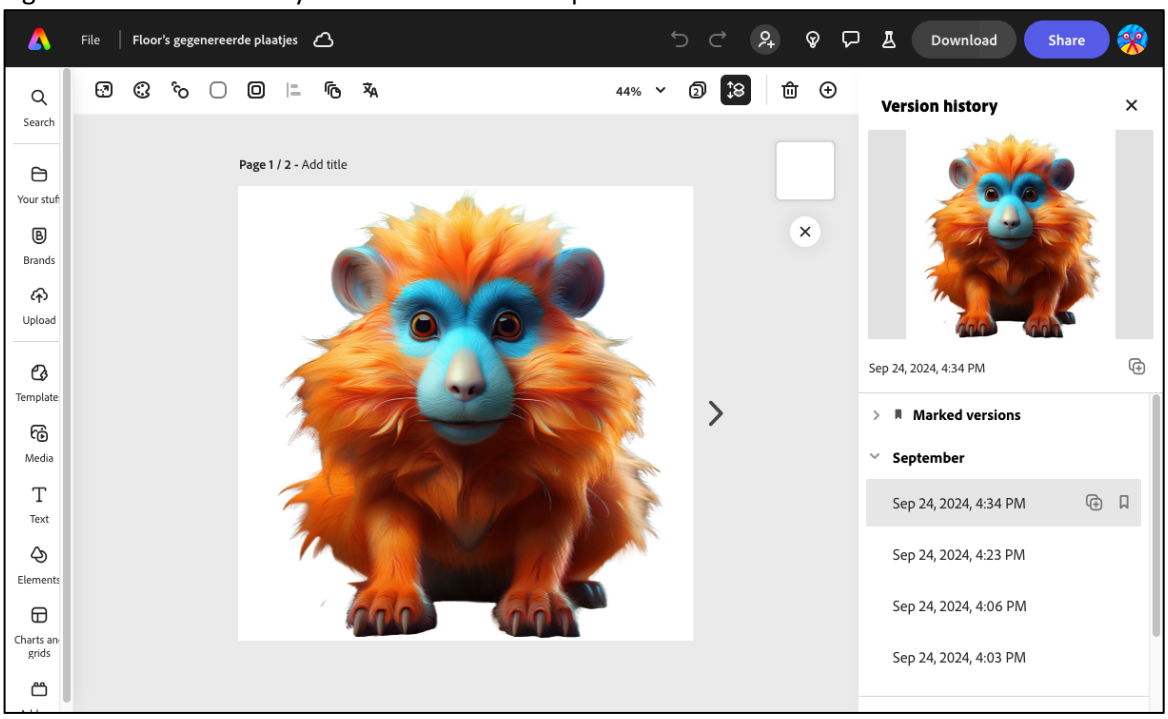
Adobe Creative Cloud Documents are versioned, and the user can request an overview of older versions from the application. The document can be restored to any of the old versions (see Figure 37).

[259] Feedback Adobe to SURF 18 December 2025.

Versions are kept for 180 days, although 60 days is mentioned in some of the application dialogs (this is probably because that was the previous retention period).[260] In case of a *marked* or *named* version, the version is kept indefinitely.[261] Users cannot choose to remove individual versions, it is only possible to remove the whole file including all versions.

Adobe Document Cloud files (as shown in Adobe Acrobat) are not versioned and cannot be restored to older versions.

Figure 37: Version history as shown in Adobe Express



3.2.3.7 Student File Transfer

Students and staff of educational institutions can use Adobe's Student File Transfer service, available at https://graduation.adobe.com, to transfer information from their educational account to a personal Adobe ID.[262] This way, they can keep access to their files when graduating. The tool performs a one-way copy of assets from the user's educational account to their personal account. It is important users use the tool before their educational account is disabled and the tool cannot be used to transfer information across geographical regions. The transfer tool supports most Adobe products (e.g., Express, Photoshop, Acrobat and Firefly are supported).[263]

[260] Adobe Creative Cloud enhancements for business plans, last updated 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/enhancements-for-business-plans.html.

[261] Versioning FAQ, last updated 5 April 2022, URL: https://helpx.adobe.com/creative-cloud/help/versioning-faq.html.

[262] Student File Transfer (formerly Student Asset Migration), last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/migrate-student-assets.html.

[263] During initial tests on 30 January 2025 and 3 February 2025 the tool did not work successfully, but Adobe since rectified this issue, email Adobe to SURF of 28 March 2025. Functionality was verified on 5 May 2025.

3.2.4 Redaction

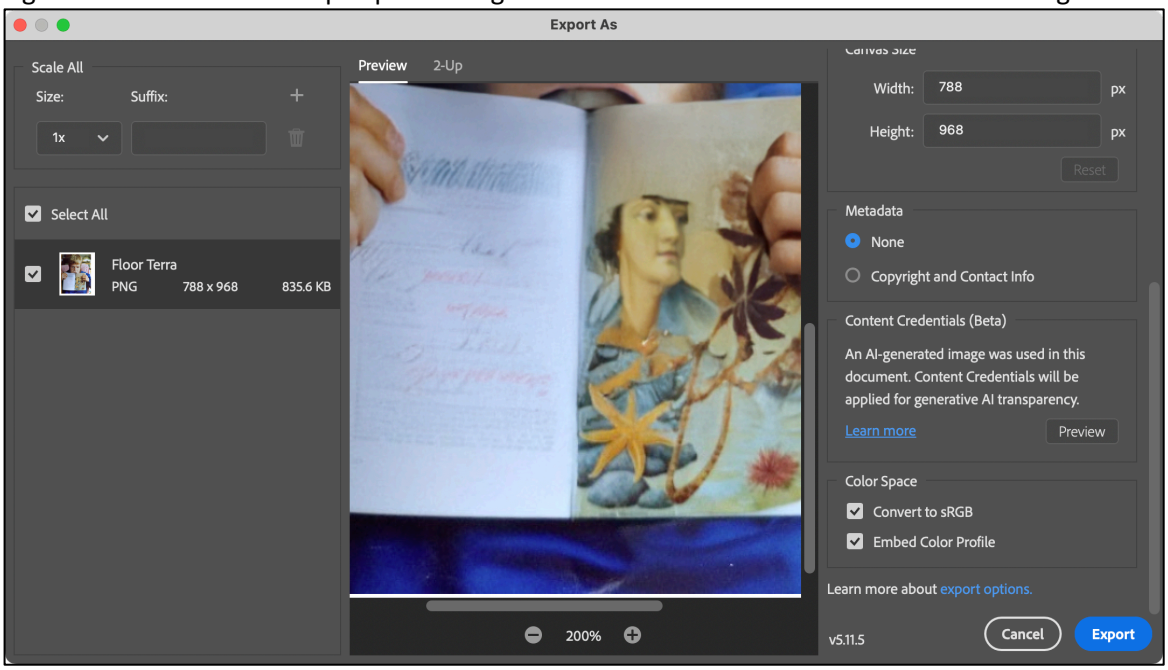
Adobe Acrobat includes redaction tools to remove sensitive or confidential information from PDF-files. Users can also search and redact based on patterns. The redacted information is completely removed from the files. When storing the document, the user is also prompted to 'sanitise' the document removing information from metadata and other hidden parts of the file.[264]

3.2.5 Exports, metadata and content credentials

Images can have *metadata* attached to them, like the author's name. When exporting an image Adobe Photoshop (desktop) gives the option to include copyright and contact information in the image metadata. This option is disabled by default. The online version of Photoshop never includes such metadata.

When AI-generated images have been used in the image, Photoshop (both desktop and web) will include Content Credentials in the image (see section 8.1.5). The desktop version of Photoshop warns about this before the image is exported (see Figure 38), the web version only mentions this after the image has been exported. During testing, Adobe Express did not attach metadata or content credentials to images.

Figure 38: Adobe Photoshop export dialog with metadata and Content Credentials settings



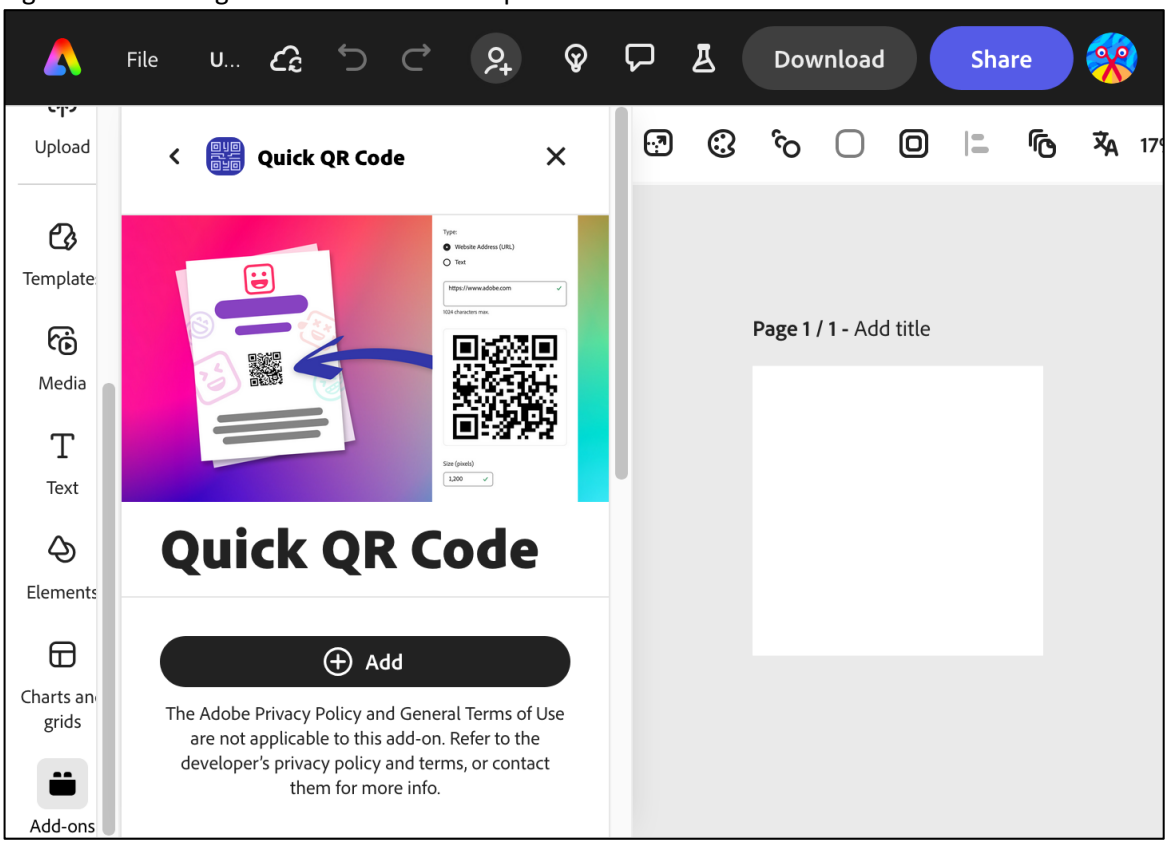
3.2.6 Integrations and add-ons

The Adobe products offer various integrations with third parties. In most cases, these integrations fall outside the scope of Adobe's privacy policies and the user is warned about this when using the integration or add-on.

[264] Adobe, Adobe Acrobat with Document Cloud Services Security Overview, p. 4, February 2024, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/doc-cloud/acrobat-dc-security-overview-ue.pdf.

Adobe Express add-ons were already discussed in the admin controls section of this document (see Section 3.1.9). End-users have to enable these add-ons themselves (if available) and are then reminded of the privacy policy of the add-on (see Figure 39).

Figure 39: Enabling an add-on in Adobe Express



Integrations are third-party solutions that use the Adobe APIs to access data in Adobe Cloud. An example of such an integration is the integration between Google Workspace and Creative Cloud, allowing access to Creative Cloud files from Gmail, Google Docs and Slides.[265] When *'installing'* an integration, the end-user will have to consent to the third-party accessing its Creative Cloud data. Admin control over integrations was discussed in Section 3.1.8.

Adobe Acrobat offers integration with third-party storage providers (Box, Dropbox, Google Drive, OneDrive and SharePoint, see Figure 40). The exact storage providers offered differ between the desktop version (all) and the web version (OneDrive, Google Drive and Box). When a third-party storage provider is connected, the storage of those third parties can be used as-if it were Adobe Cloud Storage.

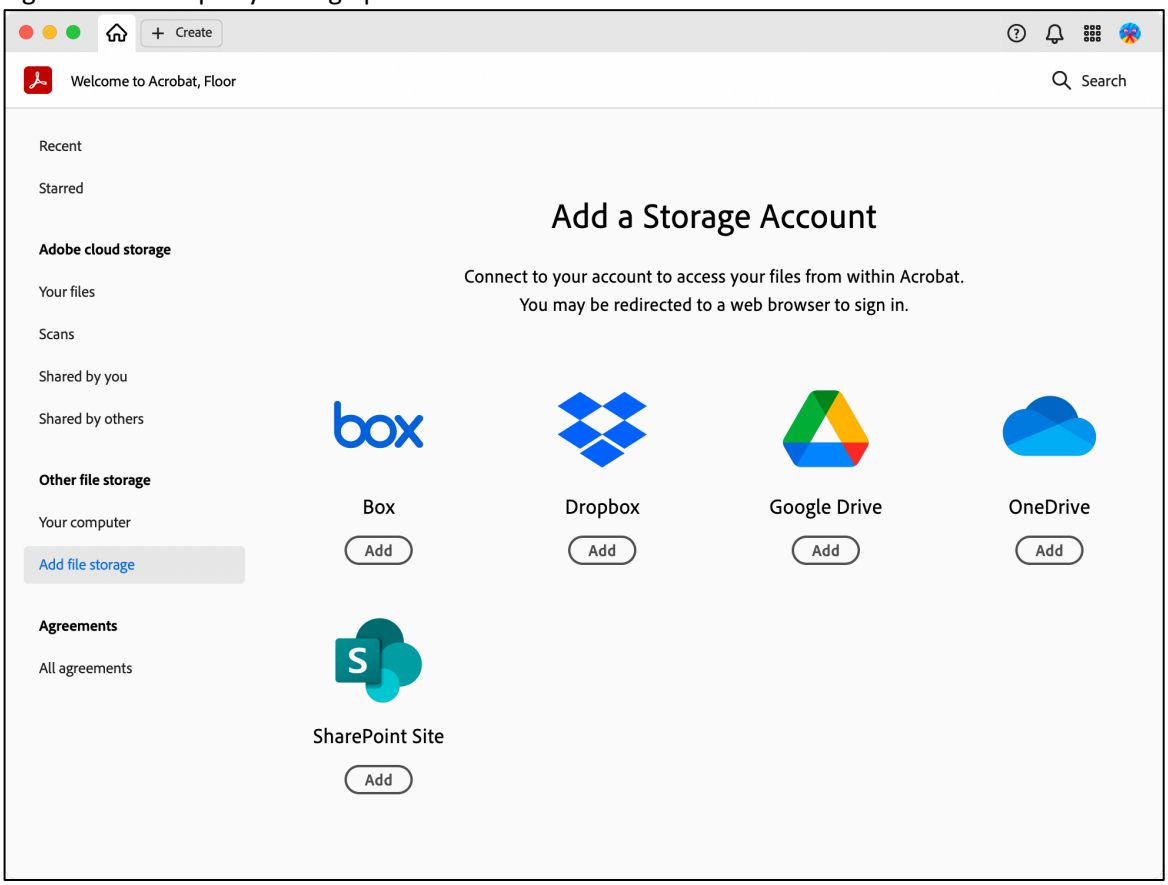
Adobe has clarified that these storage integrations cannot be disabled for the web version of Acrobat, but that administrators can disable access from the Google Drive or OneDrive settings.[266] However, this would not prevent a user from linking their personal Google or OneDrive account. For the desktop version of Acrobat, integrations can be disabled through the

[265] See URL: https://workspace.google.com/marketplace/app/adobe_creative_cloud/969673929375.

[266] Email Adobe to SURF, 14 February 2025.

Windows register.[267] This does require administrators to have administrative control over the end-user's device.

Figure 40: Third-party storage providers in Adobe Acrobat



Adobe Express allows end-users to connect their social media accounts to the product, to schedule and automatically publish content to these social networks. It is possible to connect to Facebook, Instagram, X, Pinterest, LinkedIn and TikTok.[268] Connections to social media accounts expire after 60 days and then need to be reconnected. Expiring does not remove any of the social media posts that were previously placed through Adobe Express from the social medium or Adobe Express. Users can also remove the connection from within the Adobe Express interface, in that case the previously placed posts are removed from Adobe Express, but not from the social medium.

3.2.7 Desktop-specific features and preferences

This section discusses various features and preferences that only apply to the desktop versions of Creative Cloud, Photoshop and Acrobat.

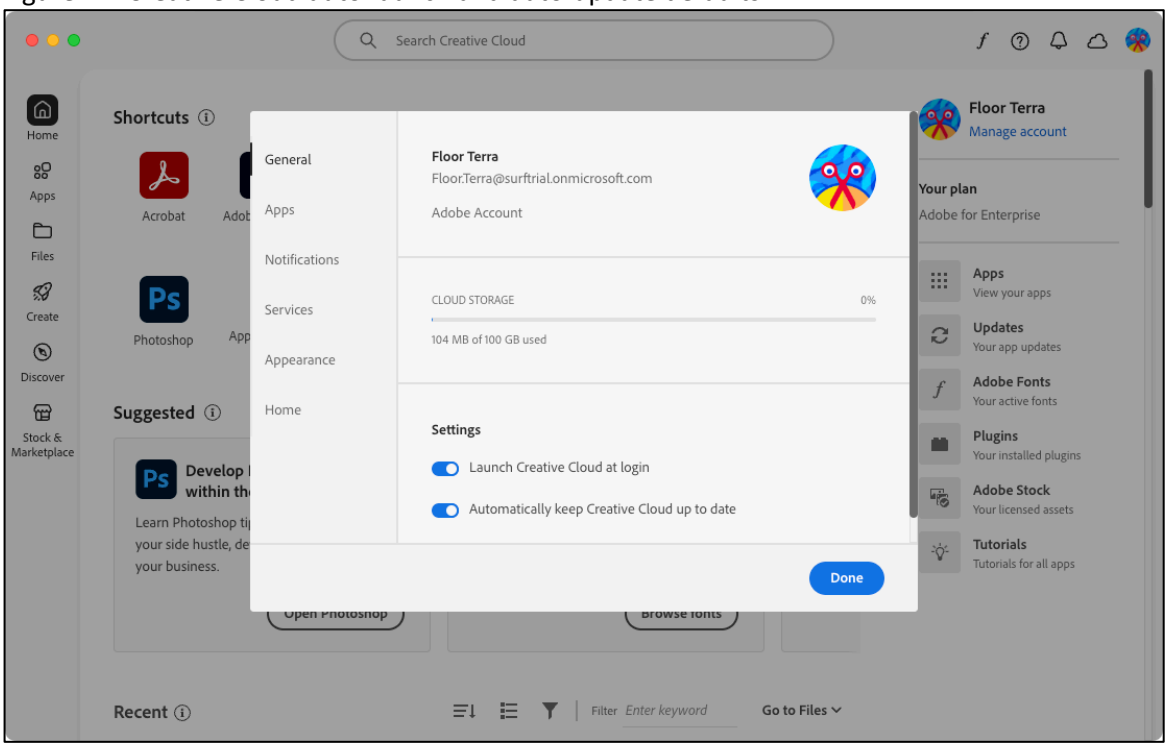
[267] Email Adobe to SURF, 14 February 2025. Control documentation available at https://www.adobe.com/devnet-docs/acrobatetk/tools/AdminGuide/sharepoint.html?highlight=sharepoint#disabling-sharepoint-integration and https://www.adobe.com/devnet-docs/acrobatetk/tools/PrefRef/Windows/FeatureLockDown.html#idkeyname_1_9921.

[268] Schedule and publish social media posts, last updated: 25 September 2024, URL: https://helpx.adobe.com/express/share-and-publish/schedule-and-publish-content/schedule-publish-social-posts.html.

3.2.7.1 Automatic launch and updates

By default, the Creative Cloud desktop application automatically starts in the background when the user logs on to the computer (see Figure 41). This can be controlled in the preferences dialog of the application. Creative Cloud and the other Adobe applications are also automatically updated by default (unless otherwise configured in the admin policies, see Section 3.1.3.3).

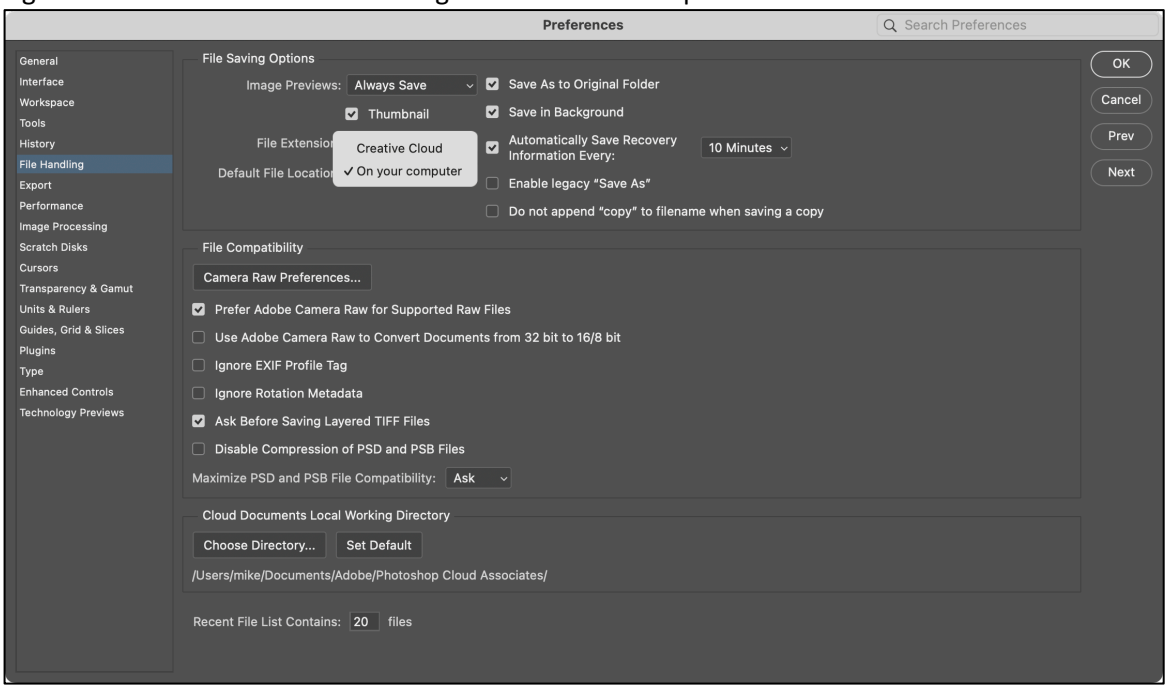
Figure 41: Creative Cloud auto-launch and auto-update defaults



3.2.7.2 Default storage location

The Photoshop and Acrobat desktop applications save to the local computer by default. For Photoshop, the default storage location can be set in the application preferences (see Figure 42). Acrobat has settings to show or hide the online storage when opening or saving file (under *'General'* in the application preferences).

Figure 42: Default file location setting in Adobe Photoshop

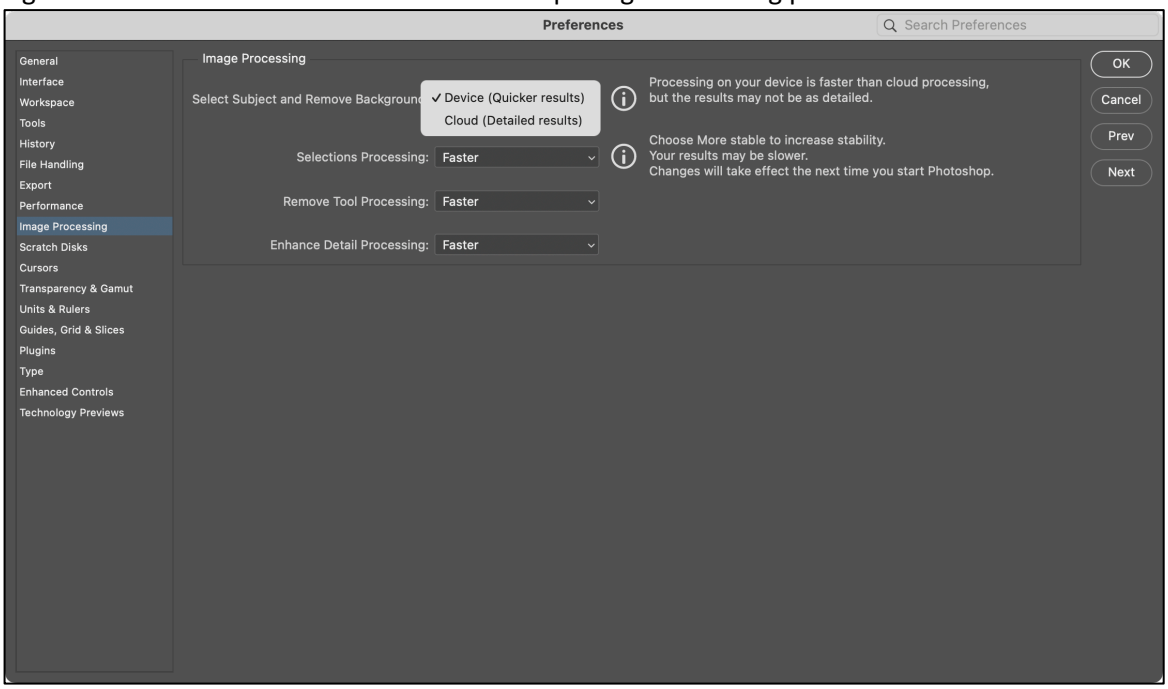


3.2.7.3 Online services

Several features in Acrobat and Photoshop connect to the Adobe Cloud to perform actions. Sometimes the user has an option to disable the online functionality or choose between a local or online implementation. In other cases, the user is not directly aware that the functionality is offered by an online service. An example of the latter is the Firefly AI functionality discussed in Section 8.1, which cannot be disabled by the end-user.

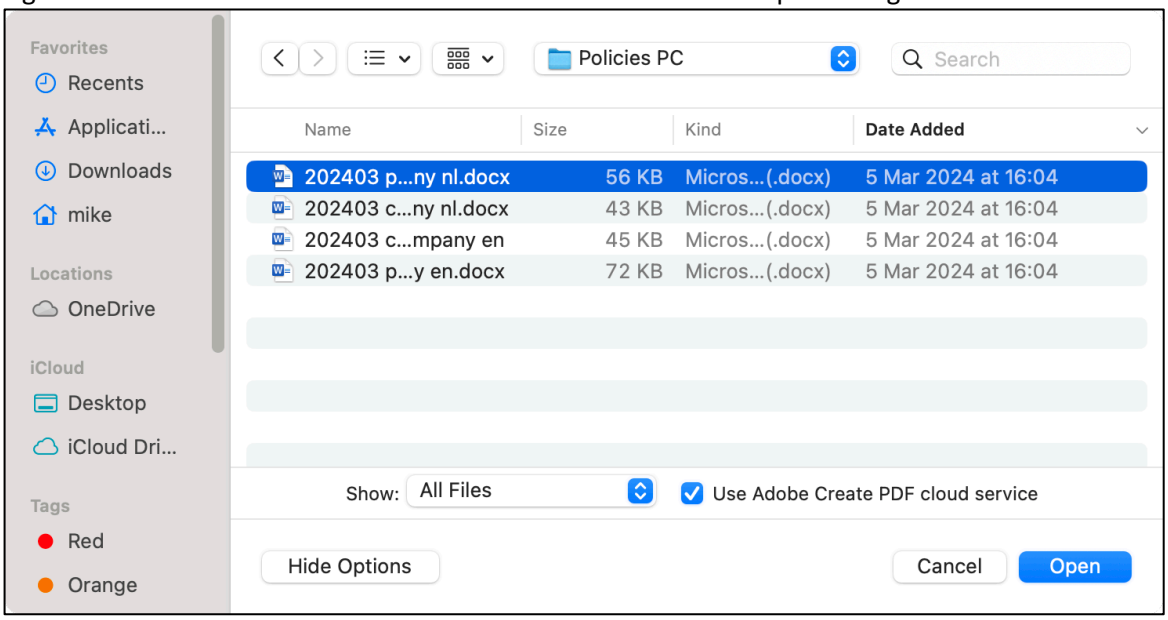
For the *'Select Subject'* and *'Remove Background'* functionalities in Photoshop, the user can choose in the preferences between a local on-device implementation or a cloud implementation (see Figure 43).

Figure 43: Device vs. Cloud choice in Photoshop Image Processing preferences



Acrobat has a setting to *'Sync preferences across devices and document services'* (under *'Adobe Online Services')*, which is enabled by default. By default, it also uses Adobe's cloud services to convert files when opening a file in a different format than PDF. This setting can be changed in the open dialog (see Figure 44).

Figure 44: Adobe Create PDF cloud service checkbox in Acrobat open dialog



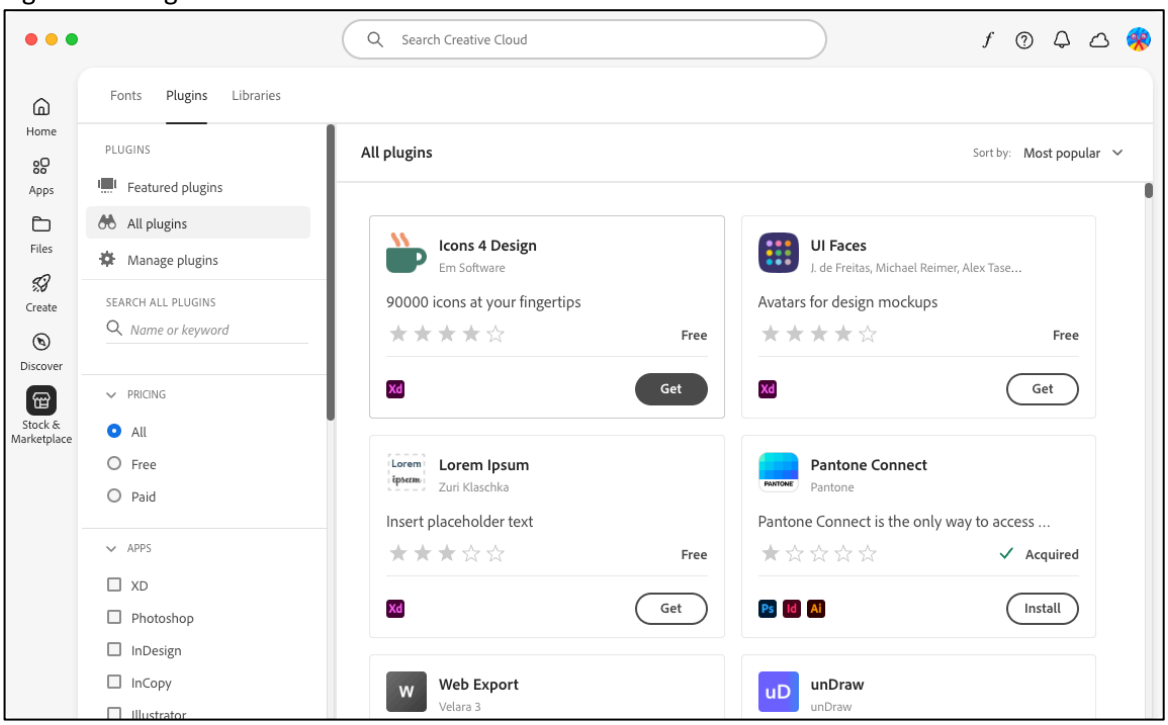
3.2.7.4 Plugins

The Creative Cloud application allows users to install plugins and extensions for the desktop applications, under *'Stock & Marketplace'* > *'Plugins'* (see Figure 45). These plugins extend the functionality of the applications with custom code of third parties. Some plugins are available for

free, others require payment by the user. Plugin management is always available to users and cannot be disabled by administrators.

According to Adobe, self-service plugin installation should not be available to educational customers.[269] Nevertheless, during testing the test users were able to install plugins and Adobe clarified this is due to the fact that self-service plugin installation is only disabled when using managed packages (see Section 3.1.4).

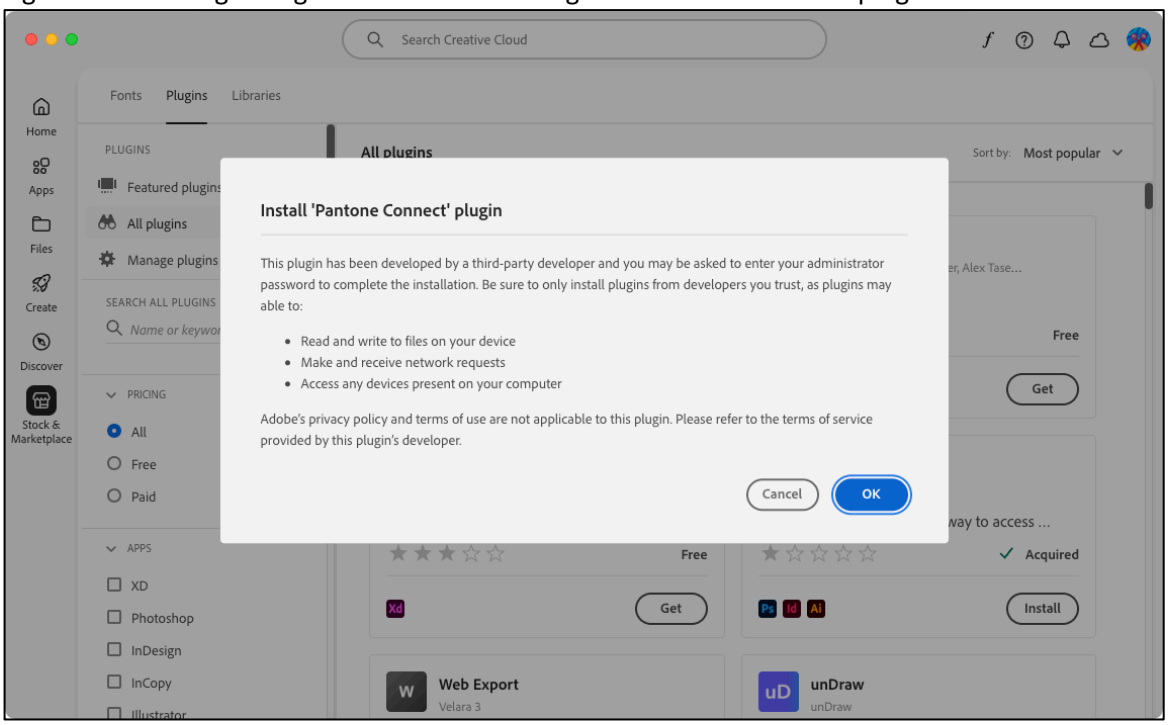
Figure 45: Plugin overview in Adobe Creative Cloud



Most plugins are provided by third parties. When installing such a plugin, a warning is shown that mentions that plugins have broad access to the user's computer and that Adobe's privacy policy and terms of use are not applicable to the plugin (see Figure 46).

[269] Email Adobe to SURF, 14 February 2025.

Figure 46: Warning dialog shown when installing the 'Pantone Connect' plugin



Update after completion of Part A

Since October 2025 "*Adobe has modified the Adobe Creative Cloud Desktop user experience so that authenticated users who are identified as students with accounts provisioned by an educational institution, such as SURF, cannot find, acquire, or install plugins from the Adobe Creative Cloud Desktop.*"[270] This update has been taken into account in parts B-D of this DPIA.

4 Purposes of the processing

Under the GDPR, the principle of 'purpose limitation' dictates that personal data may only be collected for specified, explicit and legitimate purposes, and may not be further processed in a manner that is incompatible with the initial purpose. The purposes are qualified and assessed in part B of this DPIA. This section focusses on the purposes of the processing of personal data by Adobe. The specific purposes of the data processing by Dutch educational institutions are outside the scope of this umbrella DPIA.

4.1 Permitted and prohibited uses by Adobe under the Agreement

As a processor, Adobe is only allowed to process personal data on behalf of and for the purposes of the educational institution (the data controller). The legal documentation includes clauses relating to Adobe's permitted and prohibited uses of the personal data. The following subsections outline the provisions in the various documents.

[270] Email from Adobe to SURF, 31 October 2025.

4.1.1 'Permitted use'

The following subsections describe the purposes of the processing for Adobe as data processor, and the so-called 'permitted use' of personal data by Adobe as described in the legal documentation.

4.1.1.1 Enterprise General Terms

The Enterprise General Terms[271] include a clause on the permitted use of 'Customer Data':

> *"Customer agrees that Adobe and its Affiliates may use, copy, transmit, sub-license, aggregate, model, index, store, and display Customer Data for one or more of the following:*
> *(1) to perform its obligations under this Agreement;*
> *(2) for product improvement and development;*
> *(3) to publish and distribute any anonymized information (i.e. information where neither Customer nor its site visitors are capable of being identified, which may be aggregated with other customers' anonymous information); or*
> *(4) to enforce its rights under this Agreement."*

4.1.1.2 Adobe DPA

Adobe's DPA (June 2024) includes the following clause regarding customer instructions[272]:

> *"Customer Instructions. Adobe will use, retain, disclose, or otherwise Process Personal Data only on behalf of Customer and for the limited and specific business purposes (as set out in Exhibit 1) of providing the Cloud Services and in accordance with Customer's instructions, including as described in the Agreement. Customer will ensure its Processing instructions are lawful and that the Processing of Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The Parties agree that the Agreement (including this DPA) sets out the complete instructions to Adobe for all Processing of Personal Data."*

The Exhibit 1 to Data Processing Addendum – Details of Data Processing, describes as the purpose for the processing *"the provision of the Cloud Services pursuant to the Agreement".*

4.1.1.3 Student Data Terms

Adobe's Student Data Terms also describe permitted and prohibited use of Student Data (see definition in Section 2.1.2.3). Permitted uses of Student Data are according to Adobe's Student Data Terms are listed in the table below: [273]

Table 8: Purposes / use of Student Data

Purpose	Sub purpose
Provision of the services	providing the Services as contemplated by the Terms

[271] Article 6.2, Adobe General Terms (2024v1), (2024v1), Effective Date: 8 March 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf.

[272] Article 3.4 Adobe DPA (June 2024).

[273] Article 5.2 Student Data Terms.

	maintaining, supporting, evaluating, analysing, diagnosing, improving and developing Adobe's websites, services, and applications, as permitted by applicable law
	enforcing Adobe's rights under the Terms
	as permitted with the consent of the parent, legal guardian, Adult Student, School, User, or Customer
	as otherwise authorized by applicable law.
Sharing / posting of information by the students	-
Adaptive/Customized Student Learning and Recommendations	for adaptive or customized student learning purposes
	to recommend educational products or services to parents, legal guardians, and Customer or School employees, so long as the recommendations are not based in whole or in part upon payment or other consideration from a third party.
Account maintenance	to send emails or other communications to Users relating to the operation and use of their accounts and the Services, such as to respond to the specific requests of Users, parents or legal guardians.

Regarding the sharing or posting of information by students, the Student Data Terms note that:

> *"depending on the features and functionality utilized by the Customer or School, some features of the Services may permit Users to share information or post information in a public forum, including Student Data. Customer and School administrative Users should use caution when adjusting permissions and features accessed through the Adobe Admin Console to ensure such permissions and features are configured appropriately for use by Customer, School, Students, and other Users."*

The Student Data Terms include a clause about the use of 'de-identified data'. De-identified data includes: *"(i) Student Data from which all direct and indirect identifiers have been removed such that there is no reasonable basis to believe the information can be used to identify an individual and (ii) data relating to access and use of the Services."* According to Article 6.1 of the Student Data Terms, Adobe may use de-identified data for *"any lawful purpose, including, but not limited to, the development, research, and improvement of educational sites, services, or applications; to demonstrate the effectiveness of the Services; and to inform, influence, or enable marketing, advertising, or other commercial efforts by Adobe."*

The Article then states: *"Unless permitted or required by law, Adobe agrees not to attempt to re-identify any such data. Adobe has no obligation to delete de-identified data."*

As described in Section 1.5.1.3 there is no clause establishing the hierarchy between the Student Data terms and the DPA published on Adobe's website. Adobe's Enterprise Licensing Terms, its General Terms, and Specific Product Licensing Terms are not mentioned in the Student Data Terms.

4.1.2 'Prohibited use'

Some legal documents also include provisions on 'prohibited use' of personal data by Adobe. The provisions on prohibited use in Adobe's DPA and the Student Data Terms are placed side by side in the table below to enable comparison of their similarities and differences.

As described in Section 1.5.1.3 there is no clause establishing the hierarchy between the Student Data terms and the DPA.

There is no provision about prohibited use of personal data by Adobe in the Sales Order and Adobe's Enterprise General Terms.

Table 9: Comparison provisions on prohibited use of personal data

Adobe's DPA (June 2024)	Article 5.1, Student Data Terms (Last updated June 18, 2024)
"3.5 No Combination of Personal Data; No Sale or Sharing of Personal Data. Adobe will not (i) combine Personal Data with other personal data it receives from or on behalf of another person or persons, or collects from its own interaction with an individual or (ii) process Personal Data outside of the direct business relationship between Adobe and Customer; provided, however, that Adobe may perform such combination or processing for any business purpose permitted or required under the Agreement to perform the Cloud Services. Adobe will not independently "sell" or "share" Personal Data (as such terms are defined under CCPA and other U.S. Data Protection Laws). With respect to Personal Data subject to CCPA, Customer may, with prior notice to and coordination with Adobe, take reasonable and appropriate steps designed to (i) ensure that Adobe Processes Personal Data in compliance with this DPA and applicable Data Protection Laws, which are set forth in and subject to the obligations set forth in Section 6 of this DPA regarding audit rights; and (ii) stop and	" i. No Sale or Rental of Student Data. Adobe will not sell, disclose, transfer, share, or rent any Student Data to any entity other than the Customer, School, Student, parent or legal guardian except in the limited circumstances described in the Terms.

remediate unauthorized Processing of Personal Data."	
"3.6 No Assessment of Personal Data by Adobe. Adobe will not assess the contents or accuracy of Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for making an independent determination as to whether its use of the Cloud Services will meet Customer's requirements and legal obligations under Data Protection Laws."	"ii. No Use of Student Data for Targeted Advertising or Marketing. Except as noted in Section 5.2 below, Adobe will not use Student Data: (a) to inform or direct targeted online advertising or marketing to Students or to a parent or legal guardian; (b) to amass a profile of a Student, other than for the purpose of providing the Services; or (c) for any other commercial purpose. For purposes of clarity, Customer acknowledges and agrees that Adobe may market or advertise without the use of Student Data, including (1) to parents, legal guardians, Students, and/or Customer or School employees or others, and (2) when based on the context of the domain or the content in view of a Student during a Student's then current visit to an online location; provided, that such advertising or marketing is not based on a Student's online activities collected through the Services over time."

The limited circumstances as mentioned in 5.1 of the Student Data terms are as follows:

- *"Third-Party Service Providers: Adobe may, from time to time, engage third-party service providers to supply ancillary services in support of the Student Services and may provide these third-parties access to Student Data subject to contractual privacy and data protection terms. This would not be a sale or rental however, only a potential sharing for limited purposes controlled by a strict contract and data protection measures.*
- *Change in Control: In the event that Adobe was to ever sell, divest, or transfer all or a portion of its business assets to a third party, Adobe may theoretically in such a circumstance transfer Student Data to such third party. If this were to happen it would be subject to the following: that (i) such third party agrees to maintain and provide the Student Services subject to data privacy standards no less stringent than Adobe's terms, or (ii) Adobe gives the Customer notice and an opportunity to opt out of the transfer of Student Data.*
- *Parent Access Requests: Customers may receive requests from Parents to access Student Data. Upon receiving a request, Adobe will work with Customer and its School(s) as needed to facilitate access to requested Student Data.*
- *Law Enforcement Access Requests: Should a third party, including law enforcement and government entities, contact Adobe with a request for Student Data, Adobe will redirect the third party to request the data directly from Customer, unless and to the extent that Adobe reasonably and in good faith believes that granting such access is necessary to comply with a legal obligation or process or to protect the rights, property, or personal safety of Adobe's users, employees, or others."*[274]

[274] Email Adobe 20 December 2024.

4.2 Purposes included in Adobe's Privacy Policy

Adobe's Privacy Policy describes how Adobe uses personal data for its own purposes. The purposes can range from providing products and services, to improving products and services, personalizing user experiences and content, managing customer relationships and communication, fulfilling legal and regulatory obligations, providing tailored marketing and advertising, conducting analytics and business operations, to enhancing functionality, security and technical support.

Table 10: Purposes of Adobe as data controller

Purpose	Sub purpose
Providing Adobe products and services	Registering and managing user accounts (Adobe ID)
	Verifying identity
	Processing payments and subscriptions
	Sending necessary service-related communications (e.g., payment reminders, expiration notices)
	Providing customer service and technical support
	Providing cloud storage and syncing features
	Processing user content for requested features, such as analysing and organizing photos, videos, and other content based on characteristics (e.g., facial or voice recognition), and enabling search, tagging, and grouping functionalities
	Migrating accounts under business email addresses to employer-controlled accounts
Analysing and improving Adobe products and services	Tracking and analysing user navigation and interaction with services
	Measuring and improving effectiveness of software and websites
	Analysing user-generated content for product improvement
	Performing content analytics to personalize user experience

	Using automated techniques and human review to detect technical issues and improve features
Personalizing and customizing user experience	Analysing user behaviour and preferences
	Providing tailored recommendations
	Customizing marketing communications
	Conducting surveys and market research
Fraud prevention, security, and misuse detection	Detecting and preventing fraudulent, deceptive, or illegal and abusive activity (Child Sexual Abuse Material)
	Scanning and reviewing shared and public content for intellectual property and safety issues
	Confirming software authenticity and preventing piracy
	Monitoring account security and preventing unauthorized access
Marketing and advertising	Sending promotional communications about Adobe products and services
	Analysing engagement with Adobe emails (e.g., tracking email opens and clicks)
	Displaying personalized advertisements on Adobe and third-party platforms
	Using cookies, pixels, and similar technologies to improve ad effectiveness
	Sharing user data with third parties for their marketing purposes
Providing social media and third-party integrations	Allowing social sign-ins (e.g., using Facebook or Google accounts)
	Integrating third-party tools, buttons, and content within Adobe services
	Conducting internal business analysis

Managing business operations and corporate transactions	Merging or acquiring businesses
Legal compliance and responding to government requests	Complying with legal obligations and law enforcement requests
	Investigating and responding to legal claims
	Preventing misuse of services in accordance with applicable laws

5 Controller, processor, and subprocessor

For the purpose of this DPIA, it is essential to establish what roles the different parties involved in the data processing have.

5.1 Definitions

Article 4 of the GDPR contains definitions of the different roles of parties involved in the processing of data: (joint) controller, processor 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 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.

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 GDPR sets out various obligations of processors towards the controllers for whom they process data. Article 28(3) GDPR contains specific obligations for the processor. Such obligations include only processing personal data in accordance with documented instructions from the data controller and cooperating with audits by a data controller. Article 28(4) GDPR stipulates that a data processor may use sub-processors to perform specific tasks for the data controller but only with the prior authorization of the data controller.

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.

5.2 The role of educational institutions

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

5.3 The role of Adobe

Under the Adobe DPA (June 2024), 'Customer' is the data controller and Adobe Systems Software Ireland is the data processor.[275] It follows from the definitions of Adobe's DPA that this data processor role is limited to the Customer Data.

The DPA contains the following instructions given by the data controller (the educational institutions) for the processing of personal data in Customer Data:

> *"Adobe will use, retain, disclose, or otherwise Process Personal Data only on behalf of Customer and for the limited and specific business purposes (as set out in Exhibit 1) of providing the Cloud Services and in accordance with Customer's instructions, including as described in the Agreement. … The Parties agree that the Agreement (including this DPA) sets out the complete instructions to Adobe for all Processing of Personal Data."*[276]

Exhibit 1 describes the purpose of the processing as *"the provision of the Cloud Services pursuant to the Agreement."*

According to Adobe's Privacy Policy, Adobe Systems Software Ireland is the contracting party and data controller for users residing outside of North America.[277]

5.3.1 Third parties involved in the processing

Adobe discloses the user's personal data to other Adobe group companies and "trusted vendors" (namely those that assist with security services, customer support services). Adobe also discloses personal data to other third-party data controllers (1) "with your consent (where necessary)" or (2) to provide any requested product or service (e.g., third-party integrations). Adobe can also disclose personal data for fraud prevention, safety and security purposes. [278]

Adobe's sub-processors are described in Section 5.3.1.1, other third parties are discussed in Section 5.3.1.2. Disclosure for fraud prevention, safety and security purposes are subject of Sections 1.6 and 7.3.

[275] Article 3.1 Adobe DPA, June 2024.

[276] Article 3.4 Adobe DPA, June 2024.

[277] Adobe, Privacy Policy, last updated 18 June 2024, URL: https://www.adobe.com/privacy/policy.html.

[278] Adobe Privacy Policy, 'Does Adobe disclose my personal information to others?', last updated 18 June 2024, URL: https://www.adobe.com/privacy/policy.html.

5.3.1.1 Sub-processors Adobe Cloud Services

Adobe maintains a list of Adobe's affiliates and sub-processors that may process personal data for the different Adobe Products / Services (Adobe Cloud Services) on the customer facing Adobe Cloud Services Sub-Processors webpage. The list is categorized into (1) Sub-processors who support delivery of Adobe products and services (2) Sub-processors who provide customer support services, and (3) Adobe affiliates.[279] The list is recently updated (December 2024). The previous list included more information, such as information on the duration of the processing.

The DPA contains a clause that provides Adobe with a general authorization for engaging sub-processors, including Adobe affiliates, listed on this webpage.[280]

According to Adobe's Student Data terms, *"Adobe may, from time to time, engage third-party service providers to supply ancillary services in support of the Services provided hereunder. Customer acknowledges and agrees that, provided that they have a legitimate need to access such information in connection with their responsibilities in providing services to Adobe and such access is subject to contractual data protection terms, Adobe may permit its subcontractors, service providers, authorized representatives, and agents to access Student Data."*[281]

This clause provides fewer safeguards compared to the clause in the DPA (Article 4.2), which explicitly requires a written agreement with each sub-processor that imposes data protection obligations and security measures that are materially no less protective of personal data than Adobe's obligations under the DPA.

Because both Adobe's DPA and the Student Data Terms apply to the Agreement and no hierarchy between them is defined, it creates legal ambiguity.

To receive notice of proposed changes to the lists of sub-processors the customer can subscribe to the notifications of any changes, of sub-processors locations of processing, or other additions updates to the sub-processor webpage. When subscribing to the notifications, the user agrees to receive tailored emails with updates related to the Adobe sub-processor pages by the Adobe family of companies (see figure below). The Adobe family of companies includes both Adobe entities and Adobe's acquired companies.[282]

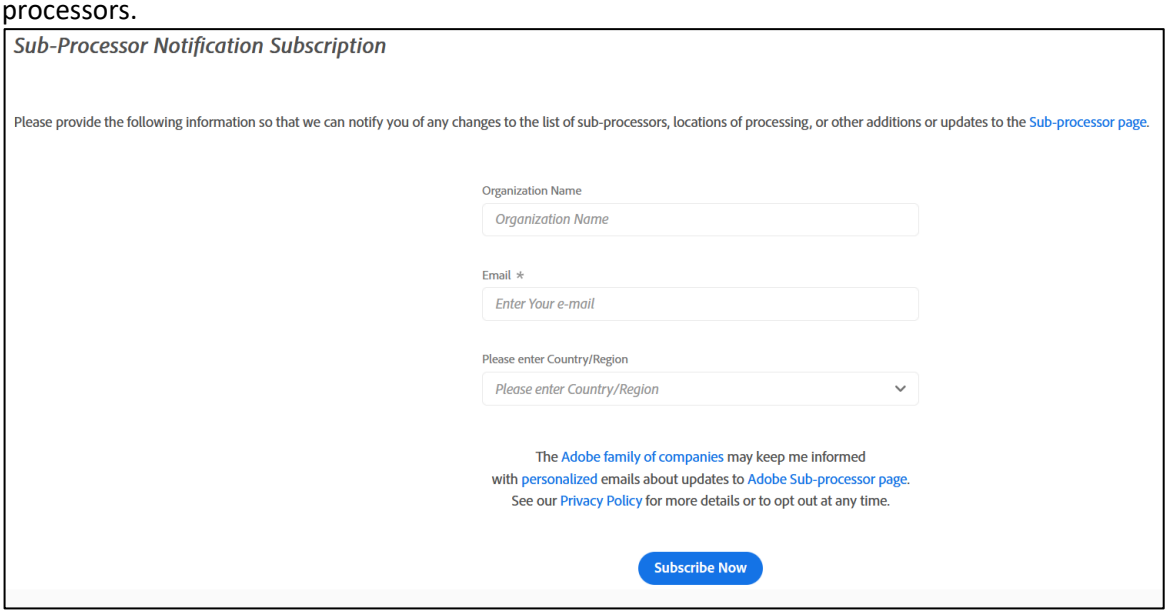
[279] Adobe Privacy Center, Adobe Cloud Services Sub-Processors, Last Updated: December 5, 2024, URL: https://www.adobe.com/privacy/sub-processors.html.

[280] Article 4.1 DPA and Article 15 (a) DPA – SURF.

[281] Article 8.1 Student Data Terms.

[282] Adobe Privacy Center, Adobe Privacy Policy, 'Does Adobe disclose my personal information to others?', URL: https://www.adobe.com/privacy/policy.html#info-share.

Figure 47: Webform to subscribe to notifications of changes or updates to the list of Sub-processors.



Adobe provides the customer with at least fourteen (14) days prior notice if the customer has opted in for the updates. Within fourteen days of such notice from Adobe the customer may object to the proposed use of an external sub-processor or Adobe affiliated party to perform the services. This objection must be provided to Adobe in writing and be based on reasonable grounds, after which Adobe will try to achieve a resolution. In case parties are not able to achieve a solution, the customer can ("as its sole and exclusive remedy") terminate the applicable sales order for the aspects which cannot be provided by Adobe without the use of the new sub-processor.

From the 31 listed sub-processors who support delivery of Adobe products and services included in the sub-processor list, the following sub-processors are relevant for this DPIA:

Table 11: Third party sub-processors providing storage and infrastructure for cloud services

Name	Adobe Products	Description	Location
Microsoft Corporation	Adobe Cloud Services, including: Adobe Creative Cloud Adobe Document Cloud	*"Microsoft Azure (Azure) provides cloud hosting services for Adobe Cloud Services (Experience Cloud, Creative Cloud, and Document Cloud). Adobe also offers the use of the Azure OpenAI service to provide features within Adobe Apps/Services where customers decide to use such features (e.g., AI Assistant in Adobe Acrobat).* *Azure is a full-service cloud platform. Data resides in Microsoft data centers but is managed day-to-day by Adobe (including strict access control protocols). For the limited categories*	USA EU UK Canada India Australia

		where Microsoft Azure can access Adobe customer data, there are strict controls applied, and all processing is subject to a range of technical and organizational measures. *For certain Adobe products, customer may have the ability to choose their primary hosting location subject to data center availability"*	
Amazon Web Services, Inc	Adobe Cloud Services, including: Adobe Creative Cloud Adobe Document Cloud	*"Amazon Web Services ("AWS") provides cloud hosting services for Adobe to host applications (including Experience Cloud, Creative Cloud and Document Cloud). AWS provides a broad suite of web service architecture to enable Adobe to manage its cloud-based products and services.* *For certain Adobe products, customer may have the ability to choose their primary hosting location subject to data center availability."*	USA EU Australia Singapore Japan
New Relic Inc.	Adobe Cloud Services	*"New Relic provides Adobe tools to help monitor overall software infrastructure and provide alerts as to telemetry data to help Adobe identify critical issues. New Relic primarily only processes technical telemetry data for Adobe (namely metrics, events, logs and traces). New Relic processes minimal personal data of customer users (e.g., IP addresses in CDN logs are used in New Relic to detect BOT traffic and bad actors in order to update firewall rules and maintain site performance)."*	USA EU

Traffic to Akamai Technologies Inc., Cloudflare, Inc., and Fastly, Inc. was observed (see Section 2.3.2.1). While these service providers appear on the sub-processor list, the products covered by this DPIA are not listed, so it is unclear from the list that these sub-processors are relevant.

Table 12: Third party sub-processors providing security for cloud service

Name	Adobe Products	Description	Location
Okta, Inc.	Adobe Cloud Services	*"Adobe uses Okta to authenticate secure access to Adobe Cloud Services. It is integrated with Adobe's cloud functions and provides provisioning, single sign-on, active directory and lightweight directory access protocol integration, centralized deprovisioning of users, multifactor authentication, and mobile identity management. Okta may process contact information (such as name, email address, and phone number), additional multi-factor authentication factor setup details, content a customer upload (such as identification or other documentation), and information regarding the websites and applications that a specific user visits when using the Okta authentication service. Okta may also receive ancillary data such as device data, usage data, and metadata. Okta's endpoint threat detection occurs on the Adobe solution stack (meaning their access to raw customer personal data is prevented)."*	USA EU UK
Splunk, Inc.	Adobe Cloud Services	*"Splunk assists with security event logging and monitoring via the collection of system data. Logs are generated through Adobe's software applications and are analyzed and inspected for bugs or system failures in an Adobe-managed Splunk environment. Splunk may process data about Adobe's operating environment and configuration. This in turn can include user interactions, and sessions related to Adobe's use of Splunk in which information and related metadata about Adobe's network and*	USA EU UK

		systems architecture configurations is accessible. From a customer data perspective, Splunk may process the number and types of searches, errors, and number of active and licensed users. Additionally, Splunk offers support services to Adobe for troubleshooting which may involve access to user/customer identifiable information. Finally, there is also a possibility of certain customer data (such as IP addresses, names, contact information,) being processed as part of a security investigation, threat detection, or incident monitoring."	
Crowdstrike Holdings, Inc.	Adobe Cloud Services	*"Crowdstrike provides endpoint threat detection as part of the Adobe Operational Security Stack (OSS). This is a monitoring solution that examines relevant devices to detect and respond to cyber threats (like ransomware and malware). It works by recording limited data points (binaries, devices, files, systems, software inventory statuses, and other data) to monitor particular sequences of events that may indicate a malicious action. Some of the information collected could potentially identify a unique user. However, this is only a remote possibility - it is extremely unlikely that customer personal data will be processed by Crowdstrike as part of this monitoring solution."*	USA
Mitto AG	Adobe Cloud Services	*"Adobe may send SMS messages to its customers for authentication, authorization and commerce flows. Mitto helps Adobe by providing SMS delivery services. To do this Mitto would have access to names, addresses, and phone numbers."*	USA EU UK Serbia

Adobe uses sub-processors who provide customer support services. The third-party sub-processors providing customer support for cloud services are out of scope for this DPIA.

5.3.1.2 Other identified third parties

Several other third parties are involved in the processing, but no information about them is publicly available, and their roles are not clearly defined in the available documentation. Adobe clarified their roles both in the DSAR response and in response to direct questions about these third parties. See the table below.

Table 13: Other identified third parties

Name	Description	Role	Purpose of the processing
Google reCAPTCHA Enterprise	*"Google provide services to prevent bot attacks, spam, and other abusive or fraudulent activities through their CAPTCHA services. They collect some basic data (IP address, device setting, browser settings, associated cookies) from users to detect whether they are genuinely human. They are not a sub-processor connected to the provision of services to customer as a controller but instead contracted directly with Adobe as our processor."*[283]	Processor	Fraud prevention, security, and misuse detection
Forter[284]	*"Forter and Arkoselab also assist on fraud prevention—identifying users via IP address and email address and verifying they are genuine. Forter is used for detecting fraudulent payment activity—they identify the use of stolen credit cards and help Adobe reject these transactions immediately. Arokoselab is focused on email addresses—when a user attempts to sign up with a high-risk email, they either get asked to use another or are flagged for further review (depending on risk profile). Again, they are not a sub-processor*	Processor	Fraud prevention, security, and misuse detection
Arkoselabs[286]		Processor	Fraud prevention, security, and misuse detection

[283] Email Adobe to SURF, 4 April 2025.

[284] Forter, Identity Intelligence for Digital Commerce, URL: https://www.forter.com/, Last viewed 20 November 2024.

[286] Arkose Labs, "Adobe Reduces Fabe Account Risk and Improves User Experience with Arkose Labs", URL: https://www.arkoselabs.com/resource/adobe-reduces-fake-account-risk-and-improves-user-experience-with-arkose-labs-case-study/, Last 22 January 2025.

	connected to the provision of services for customer as a controller but instead contracted directly with Adobe as our processor."[285]		
Branch[287]	*"Branch Metrics has provided analytics services for Adobe on how our customers are potentially using Adobe products (e.g., digital media applications such as Express and the Adobe.com website). In providing such services, Branch may process a limited amount of data on an Adobe customer's navigation of products (e.g., clicks on the Analytics Dashboards app link to strictly provide the hyperlink services or activity on a link to take the Adobe customer's user to the correct Scorecard). In doing so Branch can collect the following types of data in order for the hyperlink feature to function: IP address, User Agent, email, cookies (which are generated by Branch), org ID, company ID, and deep link ID but does not track detailed personal data (as Adobe directs this processing as a data controller). "*[288]	Processor	Analysing and improving Adobe products and services
Sentry.io[289]	*"Sentry.io is a company that provides application monitoring software to allow for the tracking of errors in real time. The data collected is related to the occurrence of software bugs (Errors) or API calls, page loads, or similar requests and responses from apps in scope (but can include IP addresses). They are not a sub-processor connected to the provision of services to customer as a controller*	Processor	Analysing and improving Adobe products and services

[285] Email Adobe to SURF, 4 April 2025.

[287] Branch, "All channels lead to you", URL https://www.branch.io/, Last viewed 20 November 2024.

[288] Feedback Adobe 4 April 2025.

[289] Sentry, "Code breaks, fix it fasters", URL: https://sentry.io/welcome, Last viewed 20 November 2024.

	but instead contracted directly with Adobe as our processor."[290]		
Fingerprint	*"Fingerprint is used during e-commerce sign up flows for necessary fraud detection by assessing browser attributes. It works by attempting to identify repeat trial users attempting to commit fraud by extending trials or signing up to new trials. It does this by running a check on the same browser via the "checkout payment page" after a user has entered payment details and produces a confidence score related solely to the technical details of the browser being used. While they are present on trial checkout flows, they should not be used specifically within products as they only work on browser attributes."*[291] *"Fingerprint is a service that Adobe uses to track users across multiple first party domains. They are not a sub-processor connected to the provision of services to customer as a controller but instead contracted directly with Adobe as our processor."*[292]	Processor	Fraud prevention, security, and misuse detection
UserVoice	*"UserVoice is a tool that allows customers to submit feedback or ideas for an improvement to an Adobe product. They are not a sub-processor connected to the provision of services to customer as a controller but instead work with Adobe."*[293]	Processor	Analysing and improving Adobe products and services

About the third-party hosting services mentioned in Section 2.3.2.8: YouTube, Vimeo and Spotify, Adobe clarified: *"although there is limited integration with YouTube on Adobe Stock concerning the measurement of ad campaigns, the cookies mentioned appear to be related to tracking privacy settings from the YouTube platform and delivering ads appropriately. The Vimeo*

[290] Email Adobe to SURF, 4 April 2025.

[291] Email Adobe 24 January 2025.

[292] Email Adobe to SURF, 4 April 2025.

[293] Email Adobe to SURF, 4 April 2025.

cookies cited are related to measuring the number of Vimeo videos watched. The Spotify cookie is linked to a podcast hosting company that ceased operations in December [2024].”[294]

6 Interests in the Data Processing

This section outlines the (potential) interests of Adobe, and the educational institutions. This section does not mention the fundamental data protection rights and interests of data subjects. How their rights relate to the interests of Adobe, the educational institutions, and is analysed in part B of this DPIA.

6.1 Interests of educational institutions

Adobe Creative Cloud and Document Cloud offer a comprehensive collection of creative and PDF tools. Educational institutions have interest in using these products as all the tools are integrated and updated regularly and work well across devices. Adobe Document Cloud services also allow for collaboration on materials across devices and users.

The Dutch education sector has an economic interest in educations students for creative and design industries. Usage of Adobe Creative Cloud services is common in many industries and knowledge of these applications is a normal and expected requirement for many employment opportunities. For instance, on 3 February 2025 Privacy Company observed the following: Searches for “photoshop[295]” and “adobe creative cloud[296]” jobs in the Netherlands on the platform Indeed yielded over 400 and 75 job postings, respectively. A search[297] for “photoshop” jobs in the Netherlands on the platform LinkedIn yielded over 50,000 results.

Schools also have a strong interest to protect children from commercial influences in the classroom. According to an agreement between schools for primary and secondary education, publishers of educational materials and the ministry of Education (Convenant "Scholen voor primair en voortgezet onderwijs sponsoring 2020-2022) all types of explicit or implicit advertising are prohibited in printed or digital learning materials or learning devices.[298]

6.2 Interests of Adobe

Adobe has a financial monetisation/economic interest in the use of the Adobe Creative Cloud and Document Cloud services. These interests are multifaceted, encompassing sales of consumer software and content, ecosystem growth, advertising potential, gathering feedback

---

[294] Email Adobe to SURF, 4 April 2025.

[295] indeed, “photoshop vacatures in Nederland”, URL: https://nl.indeed.com/jobs?q=photoshop&l=Netherlands&from=searchOnDesktopSerp&vjk=43f81485dcb81d25, Last viewed 3 February 2025.

[296] indeed, “adobe creative cloud vacatures in Nederland”, URL: https://nl.indeed.com/jobs?q=adobe+creative+cloud&l=Netherlands&from=searchOnDesktopSerp&vjk=43f81485dcb81d25, Last viewed 3 February 2025.

[297] LinkedIn, “photoshop in Netherlands”, URL: https://www.linkedin.com/jobs/search/?geoId=102890719&keywords=photoshop, Last viewed 3 February 2025.

[298] Tweede Kamer Der Staten-Generaal, Convenant "Scholen voor primair en voortgezet onderwijs sponsoring” 2020-2022, artikel 5, URL: https://www.tweedekamer.nl/downloads/document?id=6af0386c-7fb1-407d-a285-3d2b4e83d5a2&title=Convenant%20%22Scholen%20voor%20primair%20en%20voortgezet%20onderwijs%20en%20sponsoring%22%202020-2022.pdf, Last viewed 30 October 2023.

for future changes to products, and the strategic advantage of being a major player in the evolving market of generative AI products made available to consumers.

Adobe Creative Cloud and Document Cloud are increasingly incorporating generative AI services. Adobe has particular interest in establishing these services in the Dutch and, more broadly, European market. Bloomberg reported in 2023 that the market for generative AI services may grow to a 1.3 trillion USD (approximately 1.27 trillion Euro as of this writing) by the year 2032.[299] In the Netherlands, it is reported by the Centraal Bureau voor de Statistiek that, as of 2024 approximately 23 percent of people in the Netherlands have used generative AI similar to those offered by Adobe to create content. In view of this growth, Adobe has a clear economic interest in promoting use of these generative AI services in the education sector, especially as these tools become more and more standard expectations for organizations producing messaging and creative content.

Adobe sends data to third party advertisers while using these services (as mitigated by a cookie banner). Additionally, Adobe integrates third party services into the Adobe Creative Cloud, such as third-party video and audio hosting services. Adobe additionally runs internal marketing campaigns that track user activities on these services in order to market current and future products.

Adobe similarly has a business interest in operating as an independent data controller, to be able to process large amounts of data in flexible systems that enable Adobe to develop new services and features.

Adobe has a legal and economic interest to comply with the GDPR and ePrivacy rules. In its financial report for the fiscal year ending on 9 November 2024, Adobe outlines European data transfers and GDPR compliance, among other topics, as issues that may ‘impact our [Adobe’s] business model’ and ‘expose us [Adobe] to increased liability’[300].

7 Processing locations

The GDPR contains specific rules for the transfer of personal data to countries outside the EEA. In principle, personal data may only be transferred to countries outside the EEA if there is adequate protection of the personal data guaranteed. Adequate protection can be achieved in a number of ways. If the country to which data is transferred has received an adequacy decision from the European Commission, the protection can be considered equivalent to the protection within the EER. If such an adequacy decision is not present, other mechanisms can be used to ensure protection, such as applying the EU Standard Contractual Clauses (hereinafter: SCCs). For multinationals, Binding Corporate Rules may be an option for transfers between entities of the same organisation. Adobe does not have BCRs.

[299] Bloomberg, ‘Generative AI to Become a $1.3 Trillion Market by 2032, Research Finds”, URL: https://www.bloomberg.com/company/press/generative-ai-to-become-a-1-3-trillion-market-by-2032-research-finds/, Last viewed 3 February 2024.

[300] Adobe Inc., Form 10-K filed with the United States Securities and Exchange Commission, 29 November 2024, URL: https://www.sec.gov/Archives/edgar/data/796343/000079634325000004/adbe10kfy24unofficialpdf.pdf

This section describes the locations where the personal data are processed. It includes an analysis of Adobe's processing locations and factual transfers of personal data outside of the EEA in Section 7.1. Section 7.2 describes Adobe's transfer mechanisms. Section 7.3 addresses Adobe's disclosure to law enforcement and secret services.

7.1 Adobe's factual locations of processing of personal data

Adobe's corporate headquarters are in San Jose, California (United States), and Adobe has offices around the world.[301] Adobe has affiliates in the following countries: United States, Canada, India, Belgium, Czech Republic, Denmark, France, Germany, Italy, Netherlands, Norway, Romania, Spain, Sweden, Switzerland, Ireland, Armenia, Australia, Japan, United Kingdom.[302] Adobe Systems Software Ireland Limited is the contracting party for SURF.

For Firefly, Adobe states the following about the locations of processing of personal data: *"Adobe currently processes, caches and potentially stores Firefly input content in Amazon Web Services (AWS) data centers in the US-East and US-West, regardless of the user's location. Adobe Firefly stores Generation History in Enterprise Storage in the US-East, EMEA-West, and APAC-East regions. Adobe currently stores Content Credentials in AWS data centers in the US-East region, regardless of the user's location. If applicable, Adobe currently stores indemnification data in a licensing database hosted in the EMEA-West region, regardless of customer location."*[303] See also Section 8.1.1.

The DPA refers to a customer facing webpage[304] for the processing locations.[305] The webpage: Adobe Cloud Services Sub-Processors lists all Adobe's affiliates and sub-processors (see also Section 5.3.1.1) and provides general information, covering multiple services and locations, making it unclear which specific processing locations apply to the use of the services and software by the Dutch educational institutions. For example, the logs stored in the Splunk environments appear to be stored in both the EU and the US (most of the log entries – about 96% - seem to be stored in the US), see also Section 2.4.3.6.

In response to the draft of Part A of this DPIA, Adobe explains that *"[t]he public-facing sub-processor list is broken down by category and product, so only the products SURF contract for would be relevant here."*[306]

In addition to this, Adobe indicates the primary processing locations from which the sub-processor provides or delivers its applicable services. *"Primary locations are: (1) country/region where the sub-processor is headquartered and (2) any countries/regions where a sub-processor has a key processing hub outside of its headquarter country (with other potential processing locations available via the sub-processor's own documentation)."*

---

[301] Adobe, Office locations, URL: https://www.adobe.com/about-adobe/contact/offices.html, last viewed 14 November 2024.

[302] Adobe Privacy Center, Adobe Cloud Services Sub-Processors, Last Updated: April 15, 2024, URL: https://www.adobe.com/privacy/sub-processors.html.

[303] Adobe: Security fact sheet, Adobe Firefly for enterprise, Core and Web, March 2025, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

[304] www.adobe.com/go/processing.

[305] Exhibit 1, point 5 Adobe DPA June 2024.

[306] Email Adobe 4 April 2025.

The reference to Adobe's website in the DPA may raise concerns because websites are dynamic, and their content can change over time.

7.2 Adobe's transfer mechanisms

This section outlines the transfer mechanisms as used by Adobe. First it lists the varying provisions across the DPA and Student Data Terms on international data transfers in Section 7.2.1. Section 7.2.2 covers Adobe, Inc.'s participation in the EU-US Data Privacy Framework. Adobe's SCCs are discussed in Section 7.2.3. Section 7.2.4 briefly covers the DTIA's Adobe performs as data controller.

7.2.1 International data transfers handling

For Adobe's individual users and customers whose use of Adobe websites and apps results in the transfer of personal information from the European Economic Area (EEA) to non-EEA countries, Adobe relies *"on one or more of the following legal mechanisms: Standard Contractual Clauses, the European Commission's adequacy decisions about certain countries, as applicable, and consent of the individual."* [307]

For Adobe's business customers whose use of Adobe solutions involves the processing of personal information from the EEA, Adobe Systems Software Ireland Limited (Adobe Ireland) processes personal data and may transfer it to Adobe entities in non-EEA countries, such as Adobe Inc. (Adobe U.S.). Where it does so, Adobe relies on Standard Contractual Clauses (SCCs) and adequacy decisions about certain countries, as applicable, and has entered into SCCs between its relevant entities to cover these transfers. [308]

Table 14: Provisions on international data transfers

Adobe DPA June 2024 (Article 7)	Student Data Terms
7.1. General Transfer Mechanisms. If Data Protection Laws prescribe specific rules for (i) Customer's transfer of Personal Data to Adobe from a country or jurisdiction or (ii) the onward transfer of Personal Data by Adobe to a country or jurisdiction (collectively, a "Transfer Mechanism"), then Adobe will, at its discretion, use such an appropriate Transfer Mechanism."	The Student Data Terms do not include any provision addressing international data transfers.

7.2.2 Adequacy decision

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

[307] Adobe Privacy Center, Cross-border data transfers, Last updated: September 21, 2023, URL: https://www.adobe.com/privacy/eudatatransfers.html.

[308] Adobe Privacy Center, Cross-border data transfers, Last updated: September 21, 2023, URL: https://www.adobe.com/privacy/eudatatransfers.html.

and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay. With the 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.
The new EU US agreement does not change the powers from US law enforcement to compel disclosure of personal data from Dutch customers under the US CLOUD Act (Clarifying Lawful Overseas Use of Data). This act was specifically designed to obtain access to data stored in data centres in the EU. This act extends the jurisdiction of North American courts to all data under the control of U.S. companies, even if those data are stored in data centres outside the territory of the United States.

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."*

The EDPB's guidance on that risk assessment shows that controllers are allowed to assess if the relevant problematic laws in the recipient country are actually applied to the transferred data.

Adobe, Inc. has certified its participation in the EU-US Data Privacy Framework.[309] The purpose of the data collection is described as:

> *"Adobe processes personal information that it receives from its subsidiaries, customers, website visitors, and business partners in the European Economic Area (EEA). The personal information is processed in order to (1) provide the products and online services requested; (2) perform customer support activities, such as fulfilling product orders, providing technical support, and improving product offerings; (3) perform sales and marketing activities as permissible under applicable law; and (4) conduct internal business processes such as financial processing and management, fraud detection and prevention, and compliance with law. When Adobe is providing online services to its business customers, Adobe may receive and process personal information as a data processor. As a data processor, Adobe acts on the instructions from its business customers or its affiliate, Adobe Systems Software Ireland Limited, and does not control the personal information it processes. As a data processor, Adobe will only disclose personal information as instructed by our business customer or as required by applicable law. In some cases and as permitted by our customer agreements, we may disclose personal information with a subcontractor who is contracted to provide services on our behalf, in order to provide the online services to our business customers."*

[309] Data Privacy Framework List, Adobe, Inc, URL: https://www.dataprivacyframework.gov/list, last visited 25 October 2024.

If there is any conflict between the terms in Adobe's Privacy Policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern.[310]

Although Adobe, Inc. is certified Adobe has continued to rely on the SCCs for EU relevant transfers (together with Adobe's technical and organizational measures) until the DPF achieves a degree of maturity (given the history of the two predecessor mechanisms).[311]

7.2.3 Standard Contractual Clauses

Personal data may be transferred from the EEA to third countries outside of the EEA using SCCs adopted by the European Commission.[312] These clauses contractually ensure a high level of protection. The SCCs combine general clauses applicable in all cases (e.g. Section I) with (four) different modules that are adapted to different transfer scenarios. Module Two applies to data transfers from a controller (the data exporter) to a processor (the data importer). Module Three applies to data transfers from a processor (the data exporter) to a sub-processor (the data importer).[313]
Adobe relies on SCCs for international data transfers to affiliates and third-party sub-processors in third countries without adequacy decision.

Adobe provided a redacted copy of its intra-group agreement incorporating the SCCs. The headers of the articles as well as the articles that were readable demonstrate that the intra-group agreement contains the correct SCCs, including the completed Annexes, and confirms compliance with the GDPR requirements, including for sub-processors.

Adobe confirmed that with all third-party sub-processors Adobe has SCCs and has performed DTIAs for the data transfers.[314]

7.2.4 Data Transfer Impact Assessment

Adobe has published a guide to provide information for its business customers in Europe that may be performing a DTIA as part of their due diligence process in contemplation of using Adobe products and services. The guide states Adobe's summary and conclusions of its own DTIAs which it has conducted as a data exporter. The guide includes information on the following third countries: (1) Armenia, (2) Australia, (3) India, (4) Serbia, and (5) United States.[315]

Adobe Ireland is the contracting party for the educational institutions and acts as the exporter, transferring personal data to Adobe, Inc. or any subprocessors located in third countries. Therefore, the obligation to conduct a DTIA rests with Adobe Ireland.

---

[310] Adobe Privacy Policy, 'Does Adobe transfer my personal information across national borders?', Last updated: 18 June 2024, URL: https://www.adobe.com/privacy/policy.html#info-transfer.

[311] Email Adobe 4 April 2025.

[312] Based on the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 4 June 2021, URL: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf.

[313] New Standard Contractual Clauses - Questions and Answers overview, URL: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en#general.

[314] Email Adobe 13 December 2024.

[315] https://www.adobe.com/privacy/adobe-transfer-impact-assessment.html, last viewed 11 November 2024.

7.3 Disclosure to law enforcement and secret services Adobe

7.3.1 Transparency report

Adobe publishes a yearly transparency report to provide information regarding requests submitted by law enforcement, judicial authorities, and government agencies from around the world. In particular, the report provides a breakdown of the requests and whether Adobe has provided a (partial) response, and the products or services to which they relate. The last Government Requests Transparency Report is from Adobe's Fiscal Year 2023 (December 2022 - November 2023) and was last updated on 14 February 2024.[316] The report explicitly states that Adobe has not built 'backdoors' for any government – foreign or domestic – into their products and services.

According to the report, most of the legal processes Adobe has received are related to online child safety and financial fraud investigations:

- 42% (65 out of the 156 total requests Adobe received) of legal requests from the last fiscal year were follow-ups to CyberTips Adobe has sent to the NCMEC (see also Section 9.3.2).
- 35% (55 out of the 156 total requests Adobe received) related to investigations of possible fraudulent purchases of Adobe's goods or services.

To date (of the report), Adobe has not received any form of national security process, such as a National Security Letter (NSL) or Foreign Intelligence Surveillance Act (FISA) order.

7.3.2 Government and law enforcement request handling

This section outlines the varying provisions across the different data processing agreements and data terms how Adobe handle and respond to government request for data.

Table 15: Overview provisions on government and law enforcement requests

Adobe DPA June 2024 (Article 9.5)	Student Data Terms (Article 9.2)
"If Adobe receives a demand to retain, disclose, or otherwise Process Personal Data from law enforcement or any other government or public authority ("Third-Party Demand"), then Adobe will attempt to redirect the Third-Party Demand to Customer. Customer agrees that Adobe can provide information to such third-party to the extent reasonably necessary to redirect the Third-Party Demand to Customer. If Adobe cannot redirect the Third-Party Demand to Customer, then Adobe will, to the extent legally permitted to do so, provide Customer reasonable notice of the Third-Party Demand as promptly as feasible under the	*"Should a third party, including law enforcement and government entities, contact Adobe with a request for Student Data, Adobe will redirect the third party to request the data directly from Customer, unless and to the extent that Adobe reasonably and in good faith believes that granting such access is necessary to comply with a legal obligation or process or to protect the rights, property, or personal safety of Adobe's users, employees, or others."*

[316] Adobe Transparency Center, 'Government Requests Transparency Report', Last Updated: February 14, 2024, URL: https://www.adobe.com/trust/transparency/reports.html.

circumstances to allow Customer to seek a protective order or other appropriate remedy. This section does not diminish Adobe's obligations under any applicable Transfer Mechanisms with respect to access by public authorities."	

As described in Section 1.5.1.3 there is no clause establishing the hierarchy between the DPA and the Student Data terms.

8 Techniques and methods of data processing

Adobe Creative Cloud and Document Cloud are offered as SaaS-products and delivered from Adobe's Cloud Platform. The Adobe Creative Cloud portal, Adobe Express, Photoshop and Acrobat are all available as web-based versions where all data processing takes place in the cloud. On top of that, Adobe offers downloadable desktop applications for the Creative Cloud portal, Photoshop and Acrobat. These desktop applications process data mostly on the user's own computer, but use connections to the cloud for several features, like document storage and generative AI. Adobe Express is only available as a web-based product.

8.1 Adobe Firefly

8.1.1 Overview

Adobe Firefly is Adobe's family of products offering creative generative AI solutions.[317] Firefly is always on for users with a Higher Education License (HED) or a generic license. For users with a K-12 license the administrator can disable Firefly. This can be done through the optional service section of the admin controls, however this only applies to the 'Adobe Express for K-12 product'.

The Firefly functionalities are offered through several channels, including:

- A dedicated website: firefly.adobe.com
- Adobe Express
- Adobe Photoshop, both in the desktop and web versions of the applications

Firefly offers:[318]

- Generative images: generating a new image based on a text input.
- Generative fill: where an existing image surface is regenerated or filled, optionally based on text input by the user.
- Generative expand: increasing the size of images in one or more directions, optionally guided by text prompt from the user.
- Text effects: applying text effects based on a prompt from the user.
- Generative remove: remove objects from an image on user request.

[317] The Adobe Firefly product homepage is available at https://www.adobe.com/uk/products/firefly.html.

[318] Information based on the Firefly User Guide, last viewed 20 November 2024, URL: https://helpx.adobe.com/firefly/user-guide.html, and the Firefly IP Indemnification documents, last updated 14 October 2024, URL: https://helpx.adobe.com/legal/product-descriptions/adobe-firefly.html.

- Generative videos (beta): generating a video based on a text input.

Adobe Firefly was launched in 2023 as part of the Adobe Sensei suite of generative AI services.[319]

The input from the user to Firefly is:

- When modifying an image (and not generating an image from scratch): the image that needs to be modified.
- A text prompt describing what needs to be done.
- An optional reference image, to act as reference for the style of the image
- Some parameters, like a preset for the style of the image to generate and how strongly firefly should follow the reference or style.
- Effects to apply.

In an email on 31 January 2025, Adobe said about the data send to Adobe, when using Firefly, it "include things such as":

- The user's prompt instructing Adobe Firefly about the image, video, or stylized text to generate;
- The model to use in the generation process;
- Desired image aspect ratio;
- Content type;
- Composition;
- Style;
- Effects;
- Optional reference image to use in the generation process.

Firefly filters the prompt. The filter limits prompts for the following categories:

- Pornographic material or explicit nudity
- Hateful or highly offensive content that attacks or dehumanizes a group based on race, ethnicity, national origin, religion, serious disease or disability, gender, age, or sexual orientation
- Graphic violence or gore
- The promotion, glorification, or threats of violence
- Illegal activities or goods
- Self-harm or the promotion of self-harm
- Depictions of nude minors or minors in a sexual manner
- Promotion of terrorism or violent extremism
- Dissemination of misleading, fraudulent, or deceptive content that could lead to real-world harm
- Private information of others[320]

When a prompt is filtered, Firefly shows a warning that there is an issue with the prompt and ceases further action. Adobe does not publish more detailed information on the filtering in Firefly.

---

[319] Adobe Unveils Firefly, a Family of new Creative Generative AI, 21 March 2023, URL: https://news.adobe.com/news/news-details/2023/adobe-unveils-firefly-a-family-of-new-creative-generative-ai.

[320] Adobe: Product Licenses and Terms of Use, Last Updated: May 10, 2024, URL: https://www.adobe.com/legal/licenses-terms/adobe-gen-ai-user-guidelines.html

If the prompt is not filtered, then Firefly combines the prompt, reference image and other user input and passes that to the service generating the requested fill or image. This service is a generative AI model, trained with data. Firefly outputs three options, or for text to image, four options. Each of them is generated by the AI model, the user can choose one of the options and can optionally adapt the prompt for further refinements.

Which image the model outputs, is determined by the following four parameters:

1. The prompt
2. The image or part of the image to modify
3. The reference image
4. The seed

To generate the variations of the image, Firefly sets the seed for each variation to a different randomly chosen value. To recreate a generated image, Firefly reuses the seed it used previously.

Adobe stores licensing information, including the names of the users. Adobe assigns each user a GUID (globally unique identifier), which is a 128-bit text string that represents an identifier, without any other personal information and stores that GUID as part of the user's license information. Firefly uses this GUID as identifier when storing data.[321]

[321] Adobe: Security fact sheet, Adobe Firefly for enterprise, Core and Web, October 2024, URL:
https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

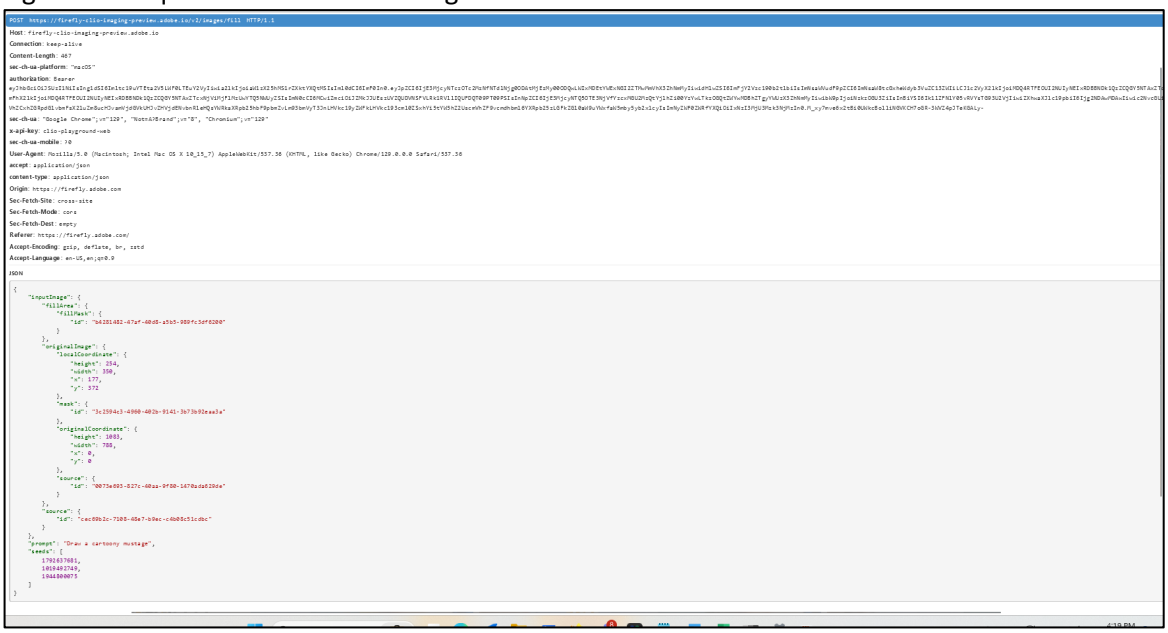
Table 16: Data storage connected to Firefly

	User prompt and configuration	Reference content	Generated content	Content credential manifest of generated content
Feedback and Ingest services	1. For 90 days, except: When selecting certain "Generative Match" functions (user gets warning first) 2. When engaging in a feedback action (e.g., rating or reporting an image), then this data is retained for max. 180 days.			
Content Credential repository				Stored indefinitely
Storage services			When saving to a library or editing in Adobe Express	
Licensing Database [322]			When downloading or exporting an image.	
Firefly	When using public sharing			
Firefly cache			Max. 24h	
Model training	Only when: Participating in user feedback program Or: Using an Adobe product which license allows AI training			

A thumbnail of the generated image, the prompt text, the seed and optionally IDs of the image to modify, fill-mask and reference image, are stored in the user's browser storage as 'Favorite image'. When requesting a 'Favorite' image, the image is recreated by Firefly with information stored in the browser:

[322] Storage in Licensing database is only active when the Adobe license includes Firefly output indemnification.

Figure 48: request to recreate an image



An example of traffic observed being sent to Firefly services during testing is included in Section 3.1.1.2.1 of the Technical Appendix.

About the locations of processing of personal data for Firefly, Adobe states: *"Adobe currently processes, caches and potentially stores Firefly input content in Amazon Web Services (AWS) data centers in the US-East and US-West, regardless of the user's location. Adobe Firefly stores Generation History in Enterprise Storage in the US-East, EMEA-West, and APAC-East regions. Adobe currently stores Content Credentials in AWS data centers in the US-East region, regardless of the user's location. If applicable, Adobe currently stores indemnification data in a licensing database hosted in the EMEA-West region, regardless of customer location."*[323]

8.1.2 Training data

Adobe states that Firefly was *"trained on a dataset of licensed content, such as Adobe Stock, along with public domain content"* and that *"you can use Firefly-generated outputs in your commercial projects"*.[324] [325]Adobe also indicates that they *"don't train on any Creative Cloud subscribers' personal content"*.[326] However, Bloomberg reported that the training data for Firefly from Adobe Stock contains images generated by the Midjourney.[327] Midjourney, in its turn, is

[323] Adobe: Security fact sheet, Adobe Firefly for enterprise, Core and Web, March 2025, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

[324] Adobe Firefly FAQ, last updated 11 September 2024, URL: https://helpx.adobe.com/firefly/get-set-up/learn-the-basics/adobe-firefly-faq.html.

[325] Adobe confirmed the statement in the FAQ about the training data in an e-mail on 31 January 2025

[326] Adobe Firefly FAQ, last updated 11 September 2024, URL: https://helpx.adobe.com/firefly/get-set-up/learn-the-basics/adobe-firefly-faq.html.

[327] Rachel Metz and Brody Ford (Bloomberg): Adobe's 'Ethical' Firefly AI Was Trained on Midjourney Images, Apr 12, 2024, URL: https://www.bloomberg.com/news/articles/2024-04-12/adobe-s-ai-firefly-used-ai-generated-images-from-rivals-for-training

trained on data that is scraped from the web without permission of the holders of the intellectual property of it.[328]

Adobe does acknowledge the importance of mitigating bias in AI and the possibility of a bias in the training data resulting in bias in the output of Firefly[329]. Adobe states: *"If (…) the AI feature points to a high risk, the product team works with the AI Ethics team throughout development to mitigate that risk. For first-party models, this may require adding data to the dataset, building additional filters, changing the algorithm, or retraining the model. For third-party models, we may build additional processes and filters in the input or output layers to help mitigate harm and bias."*[330] However, Adobe does not explain what risks or harms are considered high risks, how the risks nor the effectiveness of the mitigations are operationalised, nor does Adobe provide any information on how Adobe deals with biases that might be introduced by the operationalisation of risk, the adaption of the training set or the implementation of the filters.

Adobe points out that information on its approach to addressing bias is available in 'Our Commitment to AI Ethics':

> *"As part of developing and deploying our AI systems, Adobe seeks to mitigate bias related to human attributes (e.g., race, gender, color, ethnic or social origin, genetic or identity preservation features, religion or political belief, geography, income, disability, age, sexual orientation, and vocation). With the ultimate goal of designing for inclusiveness, we prioritize fairness in situations with significant impacts on an individual's life, such as access to employment, housing, credit, and health information. We also determine whether the advantages of using AI outweigh the risk of harm of using AI at all."*[331]

8.1.3 Generative AI Specific Terms

The generative AI features are part of the on-demand services. According to Adobe, for Firefly (Generative AI) the PSLT for Creative Cloud and Document Cloud[332] and the Firefly Product description[333] apply.[334] The PSLT give definitions for the 'input' and 'output'. Both 'input' and 'output' are Customer Content (not Content Files or Sample Files) and all provisions governing

[328] Kevin Madigan (Copyright Alliance Blog), 29 August 2024: Top Takeaways from Order in the Andersen v. Stability AI Copyright Case. URL: https://copyrightalliance.org/andersen-v-stability-ai-copyright-case/

[329] Adobe: Our Commitment to AI Ethics, October 2024, URL: https://www.adobe.com/content/dam/cc/en/ai-ethics/pdfs/Adobe-AI-Ethics-Principles.pdf

[330] Adobe: Our Commitment to AI Ethics, October 2024, URL: https://www.adobe.com/content/dam/cc/en/ai-ethics/pdfs/Adobe-AI-Ethics-Principles.pdf, p.4

[331] Adobe: Our Commitment to AI Ethics, October 2024, URL: https://www.adobe.com/content/dam/cc/en/ai-ethics/pdfs/Adobe-AI-Ethics-Principles.pdf

[332] PSLT – Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1), Effective Date: 16 Aug 2023, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-CreativeCloudandDocumentCloudSubstance3D-WW-2023v1.pdf.

[333] Adobe Firefly | Product Description, Effective as of 14 October 2024, URL: https://helpx.adobe.com/legal/product-descriptions/adobe-firefly.html.

[334] Email Adobe 13 December 2024.

Customer Content in the Agreement apply to the 'input' and 'output'[335] (see also Section 2.1.2). Restrictions apply to the 'output'. The Customer is not allowed to use the output to directly or indirectly create, train, test, or otherwise improve any machine learning algorithms or artificial intelligence systems, including any architectures, models, or weights.[336]

Adobe reserves the right to throttle, limit, disable, suspend, or terminate Customer's right to use or access the generative AI features as described in the Sales Order or in Documentation[337], as applicable.[338]

The Firefly Product description is a webpage with information about the IP indemnification and information for enterprise customers about generative credits, input, output and content credentials. Although according to Adobe the Firefly Product description is applicable, the web page states that it applies only if the link to the webpage is included in the Agreement. This is not the case for SURF. No link to the webpage is part of the Sales Order, the Sales Order Terms, and the other documents part of the Agreement. The webpage mentions twice that Adobe may update the information on the webpage from time to time.

8.1.4 Feedback and Ingest Services

The feedback and ingest services have two purposes: (1) caching of images to speed up processing and (2) storage of feedback. The cache has a retention of 24 hours. Adobe states: "*When a user uploads a reference file, such as a style reference file, a thumbnail of that reference image, along with the user identity, prompt text, and output image hash are also stored in the Feedback and Ingest Services repository*."[339]

Firefly also stores content when the user "*Engages in a feedback action (e.g., rating or reporting an image). Firefly stores the image in the Feedback and Ingest Services repository along with the user's identity information, which is used to assess and address the points raised in the feedback action (subject to the terms of the customer agreement)*."[340]

Firefly offers a feedback dialogue that the user can open after generating an image.

---

[335] Article 12.1 of the PSLT – Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1), Effective Date: 16 Aug 2023, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-CreativeCloudandDocumentCloudSubstance3D-WW-2023v1.pdf.

[336] Article 12.2 and 26 of the PSLT – Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1), Effective Date: 16 Aug 2023, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-CreativeCloudandDocumentCloudSubstance3D-WW-2023v1.pdf.

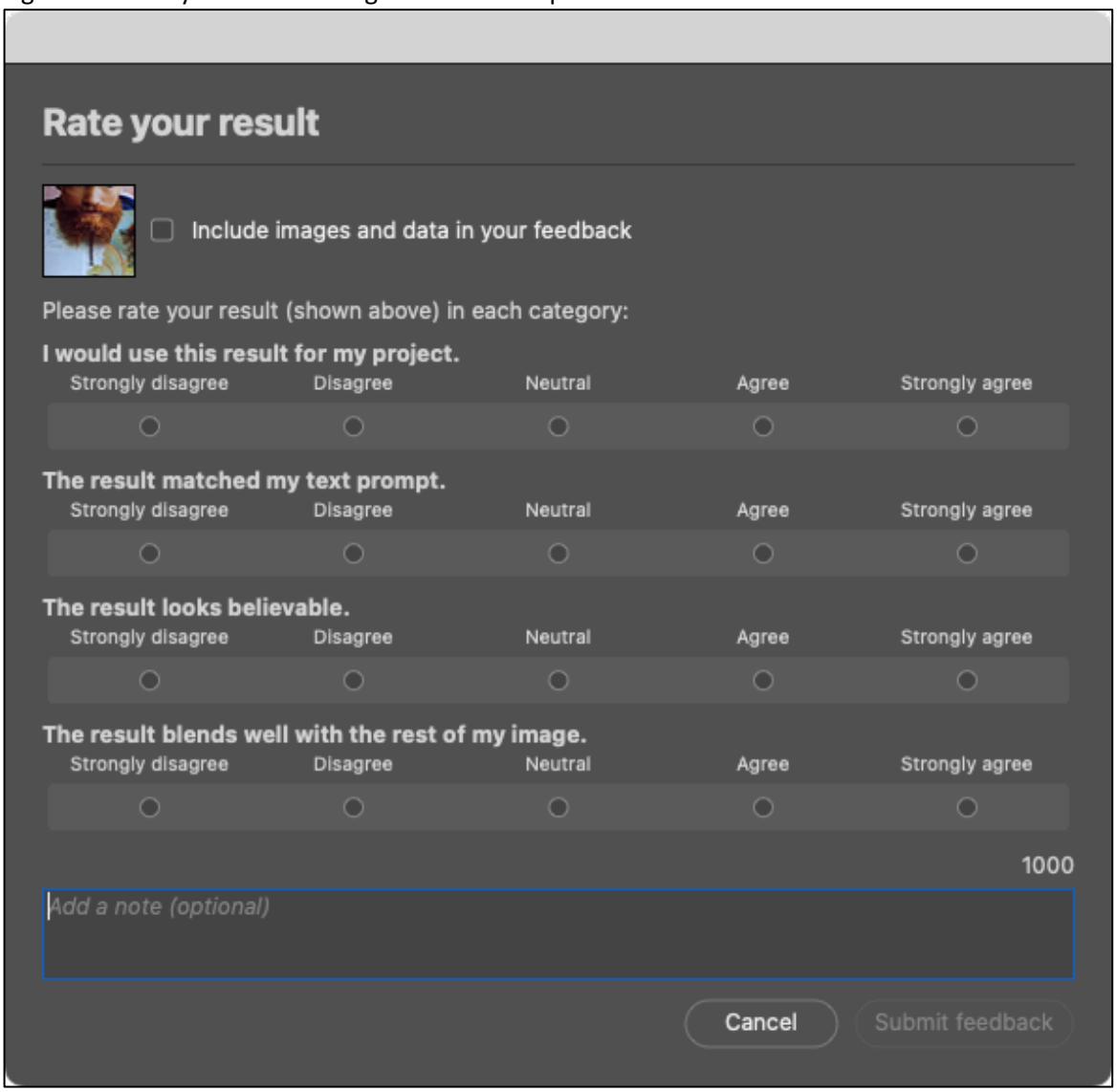
[337] "Documentation" means the applicable technical specification and usage documentation for the Products and Services as such materials are made generally available on www.adobe.com. Adobe GENERAL TERMS (2024v1), URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf.

[338] Article 12.1 of the PSLT – Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1), Effective Date: 16 Aug 2023, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-CreativeCloudandDocumentCloudSubstance3D-WW-2023v1.pdf.

[339] Adobe: Security fact sheet, Adobe Firefly for enterprise, Core and Web, October 2024, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

[340] Adobe: Security fact sheet, Adobe Firefly for enterprise, Core and Web, October 2024, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

Figure 49: Firefly feedback dialogue in Photoshop



Adobe explained:

"When a user uses Firefly, their prompt text, a thumbnail of the user-uploaded reference image (if they chose to upload one), their image configuration settings, and a GUID (e.g., i001ad83a-d41f-4afb- 9f5c- 7b72c88ae873a) are logged in the Ingest and Feedback Services Repository for 90 days, after which they are deleted.

If the user chooses to submit feedback about an Adobe Firefly image, a thumbnail of that generated image and feedback details are stored in the Feedback and Ingest Service Repository along with the data noted above in order to enable Adobe to review the feedback the user has submitted. Feedback data from enterprise users such as SURF is stored until it has been reviewed and the feedback addressed, and then for no more than 180 days. At that point, it is all deleted

or deidentified unless we are required to keep it longer for legal reasons – such as if a user were to report potentially illegal content".[341]

8.1.5 Content Credentials

Content credentials are signed information about the origin and history of an image, and these also contain a hard and a soft fingerprint of the image. This makes the content credentials tamper-free: when the image is changed after creating the content credentials, this fingerprint is not correct anymore. The content credentials are stored in the metadata of the image.[342]

When creating an image with Firefly, Firefly automatically adds content credentials to the image. Content Credentials typically contain the following metadata:

- a thumbnail of the generated image (can be switched of in some cases)
- a thumbnail of the images used to generate the image (can be switched of)
- the tool(s) used to generate the image
- summary of the actions taken in Firefly (such as use of a reference file, edit activity, etc.)
- the cryptographic fingerprint of the image[343]

Content Credentials are both attached to the exported image and are stored in the Content Credentials cloud repository, so Adobe can restore Content Credentials when they are stripped from the metadata of the image. The content credentials are retained indefinitely. Adobe did not provide any information about the purposes of the storage of the content credentials. [344] Adobe stores the global user id (GUID) with the content credentials when generating and storing the credential. This GUID is not visible when checking the content credentials.[345] .

In response to questions, Adobe clarified that the user ID is stored and used in case content is flagged as harmful content:[346]

> *"The user's ID is stored with a Content Credential when content created using an Adobe product or service is signed with a Content Credential. This information is only accessible to Adobe and is not accessible to the public through the Content Credential inspect tool. The user ID is stored in the event any content is flagged as harmful content."*

and that content credentials are stored indefinitely:

> *"Credentials are stored indefinitely to maintain the integrity of the content credential. It would be contrary to the Content Authenticity Initiative's mission of transparency regarding digital content to allow after-the-fact removal or tampering of a Content Credential."*

---

[341] Email Adobe 31 January 2025.

[342] Content Authenticity Initiative, Understanding manifests, February 2025, URL:
https://opensource.contentauthenticity.org/docs/manifest/understanding-manifest

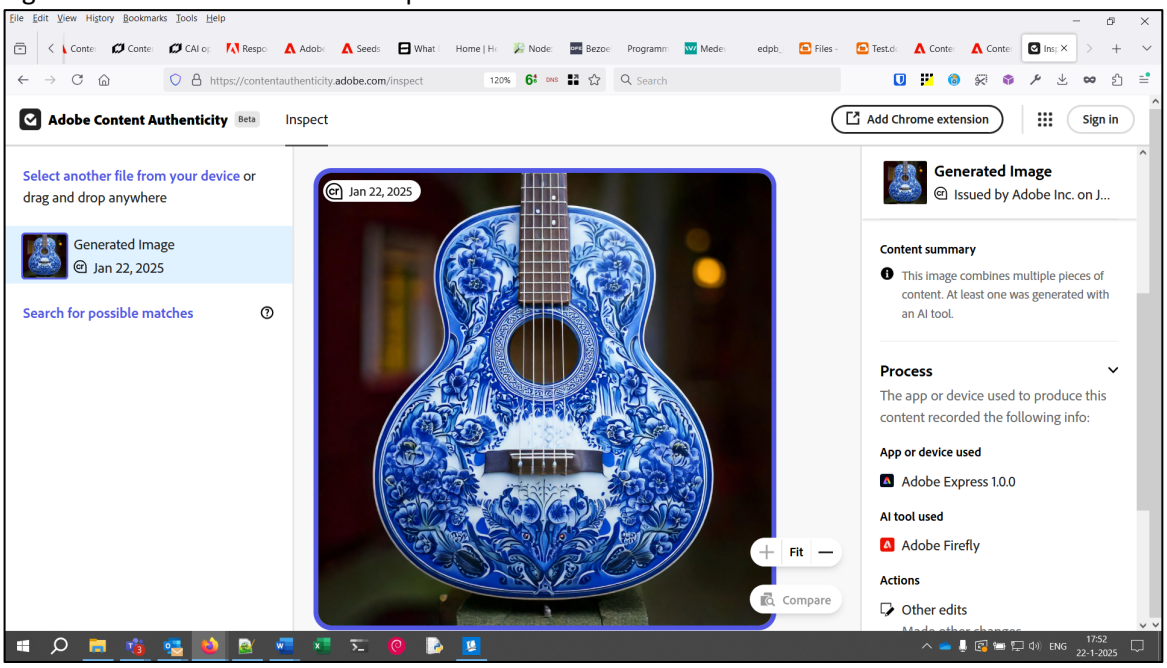
[343] Adobe: Security fact sheet, Adobe Firefly for enterprise, Core and Web, October 2024, URL:
https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

[344] Adobe: Security fact sheet, Adobe Firefly for enterprise, Core and Web, October 2024, URL:
https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

[345] E-mail from Adobe to SURF of 28 March 2025.

[346] Email Adobe to SURF, 28 March 2025.

Figure 50: Content Credentials Inspector



Content credentials can be verified in the 'Content Credentials Inspector'.[347] It is possible to upload an image to the inspector. If the image contains Content Credentials in the metadata, the inspector reads those and verifies the fingerprints. Additionally, the inspector provides the option to search for possible matches to the picture. During testing this feature did not function reliable, at most attempts it returned an error message: "Possible matches are currently unavailable". However, at some attempts it did present possible matches. The search result returned other versions of the image that were created during testing with slightly different prompts. These images were downloaded during testing but not published anywhere. Also, when searching from a browser without any cookies or active login sessions, the inspector still returned the other versions of the image. This means that anyone can find and see unpublished versions of an image. Adobe confirmed this is expected behaviour for fully AI-generated content:[348]

> *"Adobe automatically applies a Content Credential to AI-generated content created using Adobe products and services. The credential is applied when the image is generated. After a credential is applied to the image, it is added to the Content Credential public cloud, which is why when you used the inspect tool, the results included an image that was AI-generated and was a near exact match for your search."*

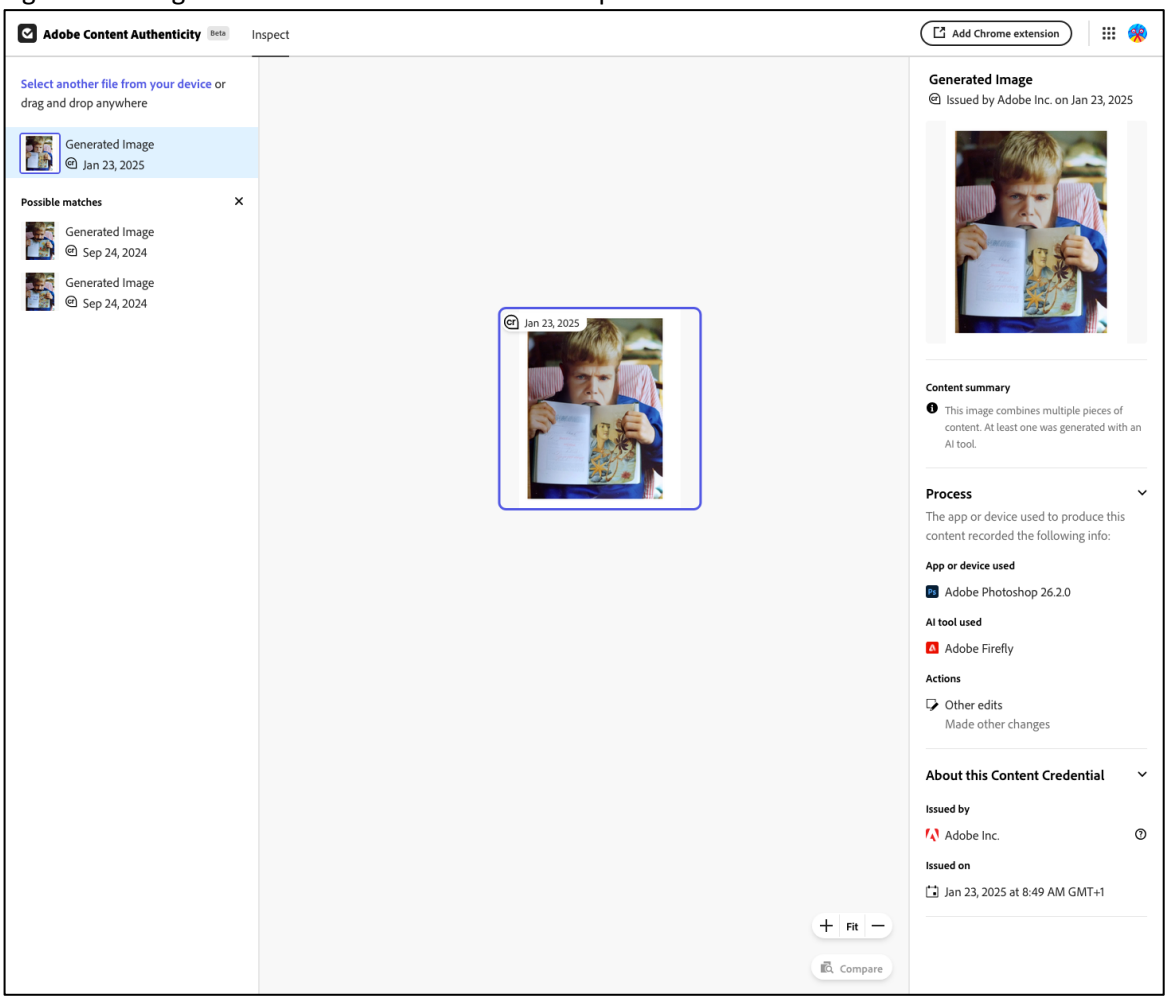
Adobe has also stated this is not expected behaviour for partially AI-generated content.[349]

[347] Adobe: Content Credentials Inspector, February 2025, URL: https://contentauthenticity.adobe.com/inspect

[348] Email Adobe to SURF, 28 March 2025.

[349] Email Adobe to SURF, 31 October 2025.

Figure 51: Image match of Content Credentials Inspector



8.2 Detection, review and reporting of CSAM

In its efforts to protect child safety, Adobe detects, reviews and reports CSAM. This section sets out what is determined in Adobe's legal and public documentation, after which the different stages of this process are described. The detection phase explores the techniques used.

8.2.1 Child Safety in Adobe's legal and public documentation

The scanning of Cloud content is mentioned in several legal documents.

The Enterprise General Terms reads:

> *"If content generated by consumers of Customer is uploaded to the Cloud Services, the following terms apply:*
>
> *A. Adobe does not review all content uploaded to the Cloud Services, but Adobe may use available technologies or processes to screen for certain types of illegal content (for example, child pornography) or other abusive content or behavior (for example, patterns of activity that indicate spam or phishing); and*
>
> *B. Adobe may access or disclose information about Customer, its consumers, or Customer's use of the Cloud Services when it is required by law or regulation (such as when Adobe receives a valid subpoena or search warrant)."*

According to Adobe's Privacy Policy, Adobe uses the collected personal data among other things

"as required by Adobe to conduct our business and pursue our legitimate interests: …

- *Analyzing your content and its characteristics using automated techniques or with human review, in the following circumstances:*
    - *Illegal and Abusive Cloud Content. Cloud Content may be automatically scanned to ensure we are not hosting illegal or abusive content, like Child Sexual Abuse Material. Human review may occur when your Cloud Content is flagged or reported as illegal or abusive."*[350]

In a blog post about Adobe's updated terms of use, Adobe explains to not scan content stored locally on the user's computer. Adobe automatically scans content users upload to Adobe's services to ensure Adobe is not hosting any Child Sexual Abuse Material (CSAM). If Adobe's automated system flags an issue, Adobe will conduct a human review to investigate. The only other instances where a human will review content of users is upon the users' request (per a support request) if it is posted to a public facing site[351], or *"to otherwise comply with the law".*[352]Adobe clarified that that the last phrase refers to the scenario in which it, as a hosted service provider, is legally required to disclose user data in response to a valid legal process issued by a government agency.[353]

Adobe's Harmful Content policies may be considered more conservative than the cultural norms in The Netherlands. However, Adobe confirmed that an image removed for violating Adobe's terms would not be reported to NCMEC unless it was CSAM (as per the US law legal definition, which applies a general standard).[354]

8.2.2 CSAM detection

Adobe scans uploaded images and videos for matches with known CSAM. (see Section 1.6 Child Safety and 3.1.11 Content logs).

Adobe uses several methods to detect CSAM: (1) hash-matching (fingerprinting) technology, and (2) machine learning models. In addition, end-users or third parties can manually flag assets for illegal content using the 'Report abuse' menu in the software.

Three elements are needed to be able to scan for CSAM by fingerprint:

1. A method to create a 'fingerprint' from a photo or video.
2. A database with 'fingerprints' of known CSAM.
3. A method to compare 'fingerprints'.

---

[350] Adobe Privacy Policy, 'How does Adobe use the information it collects about you, and what are the legal bases for these uses?', last updated 18 June 2024, URL: https://www.adobe.com/privacy/policy.html.

[351] Adobe clarified in an email to SURF of 28 March 2025 about a public facing site that *"This term is used in this context to mean services that allow for public posting of content – Adobe Behance, Adobe Stock, Adobe InDesign – as opposed to content stored in private storage such as Document Cloud"*.

[352] Adobe Blog, 'Updating Adobe's Terms of Use', 10 June 2024, URL: https://blog.adobe.com/en/publish/2024/06/10/updating-adobes-terms-of-use.

[353] Email Adobe 29 March 2025.

[354] Feedback Adobe 18 December 2025.

The hash-matching methods Adobe uses include Microsoft's PhotoDNA[355] and YouTube's CSAI Match[356] to compare digital signatures (or "hashes") of images and videos uploaded by any Adobe user to Adobe's servers against the databases of known CSAM hashes and fingerprints from the National Center for Missing and Exploited Children (NCMEC) and Google. [357]

Adobe's machine learning models uses software provided by Thorn [358]. The latter is an image-based classifier trained on a dataset of known CSAM and negatives. The machine learning classifier works with a probability score. Only images with a 'very high' probability score are flagged for further review.

Adobe self-hosts all the software and databases. Hash databases are regularly refreshed from the source.

8.2.2.1 NCMEC CSAM database

Adobe cooperates with the National Center for Missing and Exploited Children (NCMEC), a US-based private nonprofit organisation established by the United States Congress.

Adobe reports found CSAM material to NCMEC, but the NCMEC also maintains a database of known CSAM. This database contains over 325,000 unique videos and over 213,000 unique images. The database contains for each of these a PhotoDNA fingerprint. Optionally it can contain classical hash (MD5 and SHA1) fingerprints. For videos it can optionally contain a Videntifier fingerprint, but Adobe has clarified it does not use Videntifier.[359] When using the NCMEC CSAM database for scanning, Adobe downloads the fingerprints stored in the database, calculates its own fingerprint and compares those two fingerprints. This whole operation is performed by Adobe on the servers of Adobe.

Adobe has not stated whether or not it uses traditional hashes. However, the classical hashes MD5 and SHA1 are one of the type of hashes that is supported by NCMEC CSAM database.[360] These hashes create a fingerprint that is unique for a photo or a video as a whole. Each exact copy of a photo or a video has the same hash, an approximately 40 digit long hexadecimal number. Because of the length of the hash, the chance of two photos or videos having the same hash is nihil. This makes it possible to compare the hashes of two pictures to determine if the pictures are exactly the same. The downside of these classical hashes is that even the tiniest change in the picture (like changing the colour of one pixel with 1%) results in a totally different hash value. This makes it very easy to evade detection when the scanning is based on classical hashes.

8.2.2.2 PhotoDNA

Adobe confirms it uses PhotoDNA as hash technique and the NCMEC CSAM database contains a PhotoDNA fingerprint for each photo and video. PhotoDNA[361] is a perceptual hash, it calculates

[355] Microsoft, PhotoDNA, URL: https://www.microsoft.com/en-us/photodna, last viewed 15 November 2024.

[356] YouTube CSAI Match, URL: https://www.youtube.com/csai-match/, last viewed 15 November 2024.

[357] Adobe: Adobe's Commitment to Child Safety, June 18, 2024, URL: https://www.adobe.com/trust/transparency/child-safety.html

[358] Thorn, URL: www.thorn.org.

[359] Email Adobe to SURF, 28 March 2025.

[360] National Center for Missing & Exploited Children: Hash Sharing API Technical Documentation URL: https://hashsharing.ncmec.org/npo/v2/documentation/#schemas (retrieved 18 February 2025)

[361] Wikipedia: PhotoDNA, URL: https://en.wikipedia.org/wiki/PhotoDNA (last visited: 18 February 2025)

the hash value based on visual properties of the photo or video. PhotoDNA extracts contours in the picture or video and then analyses how these contours relate to neighbouring contours. It transforms these relations to a series of numbers that encode these contours. These numbers can be seen as an arrow pointing in a certain direction. Even when the picture or video is converted to another format, when the colours are transformed, when it is cropped or when for example a logo of text is added, then the arrow will still point in roughly the same direction. This enables matching, even when the pictures or videos are processed in different ways. The downside is that the matching is not exact: photos and videos that are processed in different ways, will have a slightly different arrow. When matching on basis of PhotoDNA, a cut-off point needs to be determined. This cut-off point determines if two photos or videos are considered the same or not. As a result, this cut-off point also determines the percentage of false positives and the percentage of false negatives.

8.2.2.3 Google CSAM database and CSAI Match

Adobe confirms to use CSAI Match. CSAI Match is a system for matching videos containing CSAM. CSAM Match is created and operated by Google. Google also maintains the database of CSAM. The process of CSAM Match starts on the servers of Adobe. There Adobe runs a program that Google provided in binary format and that calculates a fingerprint. Adobe then sends this fingerprint to Google and Google determines if it matches with known CSAM. Google then returns to Adobe if the provided fingerprint has a match in their database.[362] Google did not publish open documentation on the methodology of calculating the fingerprint nor on the methodology of matching fingerprints. Google does not publish any openly available information on the composition of the content of the CSAI Fingerprint repository.

8.2.2.4 Notice-and-action mechanisms

Adobe's feedback mechanism allows individuals to report content they consider illegal. This is not restricted to reports of suspected CSAM. Individuals also have the ability to report content they find abusive or illegal through Adobe's feedback mechanism. With regards to CSAM, this allows for individuals to directly report to Adobe content they believe to be CSAM. Under Article 16 of the DSA, hosting providers must establish easy-to-access, user-friendly mechanisms for submitting notices on illegal content. This feedback system fulfils Adobe's DSA obligations.

8.3 Review process

Adobe's Trust and Safety team reviews, reports, and removes CSAM discovered by Adobe's machine learning models and hash matching technology, as well as by user reports or account investigations.[363]

Each flagged asset (from PhotoDNA, Google CSAI match, Thorn or manual reporting) is reviewed by a small review team, part of Adobe's Trust and Safety team. The review queue is prioritised on the probability score (from Thorn) if available and is otherwise not prioritised. The internal SLA for review is 48 hours, and the review team can be scaled up with a backup team if necessary.

---

[362] Google: Discover our child safety toolkit, URL: https://protectingchildren.google/tools-for-partners/#testimonials (retrieved 18 February 2025)

[363] Adobe, 'Adobe's Commitment to Child Safety', last updated: 18 June 2024, URL: https://www.adobe.com/trust/transparency/child-safety.html.

8.4 Reporting process

Adobe reports all confirmed CSAM to the NCMEC as required by US federal law.[364] Content that is confirmed by manual review to be 'legally reportable CSAM' according to the US-definition of CSAM is reported to NCMEC. The team has been trained for this definition. This definition is used by Adobe for all matches and NCMEC serves as the 'clearing house' to communicate matches to other countries/parties. There are also no differences between US States. According to Adobe the US-definition of CSAM is understood to align well with most other countries.

The information shared with NCMEC is the information that is required under US law. This includes at least:

- Uploader information: name, basic subscriber information, billing information and IP addresses.
- The image itself.

In case of imminent risk of harm Adobe may share additional information.

There are no exceptions to the reporting to NCMEC. All confirmed matches are reported without further balancing test. NCMEC sends aggregated feedback and statistics on the quality of reports. These reports are confidential. Adobe has been highly rated in comparison to other software providers.

8.5 Further steps

Adobe deactivates the account of users where CSAM has been detected. The school (if applicable) is informed that the user had a Terms of Use violations, but no further information is shared.

Adobe informs the user automatically about the appeal process and allows the user to submit an appeal in an easy way. Using a free text field the user can provide contextual information or other relevant information for the appeal. Appeals are reviewed by a different team of reviewers than the team that did the original verification.

9 Additional legal obligations

This section describes the additional obligations arising from the current ePrivacy Directive and (possible) future e-Privacy Regulation. Considering Adobe's Child Safety policies and proactive scanning content for CSAM, Online Child Safety Legislation is discussed in Section 9.3. As Adobe's Student Data Terms (applicable for educational institutions) refer to certain US legislation, the applicability of this legislation is subject of Section 9.4. In view of the limited scope of this DPIA, other legal obligations or frameworks (for example in the area of information security, such as BIO) are not included in this report.

9.1 E-Privacy 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

[364] US federal law only includes the obligation to report, not to scan, see also Section 9.2.2.

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)[365], 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 e-Privacy 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. As the inter-institutional negotiations on the proposed CSAR have not concluded, a proposal for an extension of the Interim Regulation was submitted on the 30th of November 2023 to extend the derogation until 3 August 2026. [366]

9.2 Digital Services Act

The Digital Services Act (DSA) governs online services with the primary objective of ensuring a safer digitals environment that protects fundamental rights. The DSA addresses issues such as illegal content. Under Article 15(1) of the DSA, providers of intermediary services, such as Adobe, must publish at least once a year, clear and easily understandable reports on the content moderation actions they carried out during the relevant period. Article 16 establishes the rules for notice-and-action mechanisms, determining how platforms receive and process user notifications of illegal content. Article 8 clarifies that the DSA does not impose a general monitoring obligation.

[365] 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

[366] 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.

9.3 Online Child Safety Legislation

9.3.1 Child Sexual Abuse Regulation (CSAR)

The Regulation to Prevent and Combat Child Sexual Abuse (CSAR)[367] is a European Union regulation proposed by the European Commissioner for Home Affairs Ylva Johansson on 11 May 2022. The CSAR aims to create a comprehensive, long-term basis for combating online child sexual abuse across the EU. It includes mandatory risk assessments for service providers, requirements to deploy detection technologies (bypassing end-to-end encryption), and mechanisms for user redress. The proposal has faced significant controversy, particularly regarding client-side scanning and chat control, and its potential impact on privacy and encryption.

The Netherlands has recently decided (October 2024) to refrain from taking a position and to actively make this known, as the governments' concerns about the protection of fundamental rights at stake are fundamental, particularly in the areas of privacy and mail and telecommunications secrecy, and the security of the digital domain have not been sufficiently addressed at this time. The Netherlands will thus be counted among the countries that do not support the general orientation.[368]

9.3.2 US Online Child Safety Legislation

Currently there is no federal law in the US explicitly requiring service providers to actively monitor or scan user content for CSAM. The primary law in effect is 18 USC § 2258A[369], which mandates that electronic service providers who become aware of CSAM must report it to the NCMEC through its CyberTipline. The statute does **not** mandate proactive monitoring or scanning. Actually, the law explicitly ensures that providers are not required to monitor users, their communications, or actively search for illegal content in 18 USC § 2258A (f) - Protection of Privacy. This provision protects user privacy while clarifying that providers' responsibility is limited to reporting CSAM only when they become aware of it.

In case Adobe becomes aware of an apparent violation of the law that involves child pornography, the report to the NCMEC should include relevant details to aid in preventing future child sexual victimization. At the sole discretion of the provider, this may include identifying information about the involved individual, such as email, IP address, or other identifiers. Additionally, historical details on when and how the content was uploaded, transmitted, or discovered should be provided, along with geographic location data if available. Reports should also contain any visual depictions of apparent child pornography and the full communication, including associated data, transmission details, and attached files.[370]

After reviewing the report, NCMEC forwards it to appropriate law enforcement agencies for further investigation. This may include US federal agencies handling child sexual exploitation, kidnapping, or enticement crimes, as well as state or local law enforcement involved in such

[367] European Union, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN.

[368] Tweede Kamer der Staten-Generaal, Vergaderjaar 2024-2025, 34843-113, 1 October 2024, URL: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2024D35954&did=2024D35954.

[369] URL: https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2258A&num=0&edition=prelim.

[370] 18 U.S. Code § 2258A(b) - Contents of Report.

cases. Additionally, reports may be shared with designated foreign law enforcement agencies that have established relationships with US authorities like the FBI, ICE, or INTERPOL.[371]

There are several legislative efforts (proposals) to combat CSAM, such as the STOP CSAM Act[372], and the EARN IT Act[373]. The EARN IT Act, if passed, would remove certain protections for interactive computer service providers and enable these providers to be civilly and criminally liable *"regarding the intentional, knowing, or reckless advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material."*[374]

In a Public Service Announcement of the Federal Bureau of Investigation (FBI) the FBI warns that child sexual abuse material (CSAM) created with content manipulation technologies, to include generative artificial intelligence (AI), is illegal. *"Federal law prohibits the production, advertisement, transportation, distribution, receipt, sale, access with intent to view, and possession of any CSAM, including realistic computer-generated images."* The announcement includes examples of recent cases involving individuals having altered images into CSAM and explicitly mentions incidents of teenagers using AI technology to create CSAM by altering ordinary clothed pictures of their classmates to make them appear nude.[375]

9.4 US Federal and State Laws

US federal and state laws are referenced throughout various legal documents.

9.4.1 Governance Enterprise Licensing Agreement

The agreement is governed by and construed under the laws of the state of California. [376]

> *"This Agreement is governed by and construed under the laws of the state of California, without regard to any conflict of law rules or principles and excluding the application of the United Nations Convention on Contracts for the International Sale of Goods. The Parties irrevocably submit to the exclusive jurisdiction of the courts of competent jurisdiction in the County of Santa Clara, State of California, provided however, Adobe will have the right to pursue Claims against Customer in any other jurisdiction worldwide to enforce its rights under this Agreement or to enforce its intellectual property rights."*

No other provisions regarding governing law or venue are included in SURFs Sales Order.

9.4.2 Applicable US federal and state laws – Student Data Terms

The applicable Student Data Terms include a clause in which *"Each party agrees to uphold its responsibilities under applicable federal and state laws governing Student Personal Information,*

---

[371] 18 U.S. Code § 2258A(c) - Forwarding of Report to Law Enforcement.

[372] S.1199 - STOP CSAM Act of 2023, URL: https://www.congress.gov/bill/118th-congress/senate-bill/1199.

[373] H.R.2372 – EARN IT Act of 2023, URL: https://www.congress.gov/bill/118th-congress/house-bill/2732/text?s=1&r=1&q=%7B%22search%22%3A%22earn+it+act%22%7D.

[374] The Alliance for Citizen Engagement, Pros and Cons of the EARN IT Act 2023-2024, by Mark Mallet, 5 August 2024, URL: https://ace-usa.org/blog/research/research-criminaljustice/pros-and-cons-of-the-earn-it-act-of-2023-2024/.

[375] FBI, Public Service Announcement, Alert Number: I-032924-PSA, 29 March 2024, Child Sexual Abuse Material Created by Generative AI and Similar Online Tools is Illegal, URL: https://www.ic3.gov/PSA/2024/PSA240329#fn1.

[376] Article 14.2 Adobe General Terms (2024v1), (2024v1), Effective Date: 8 March 2024, URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf.

including, but not limited to, state student privacy statutes, the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g, the Protection of Pupil Rights Amendment ("PPRA"), 20 U.S.C. § 1232h, and the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6502, and the regulations promulgated under each of FERPA, PPRA and COPPA."[377] Article 20.2 of the Consortium Member Enterprise Term License Sales Order also includes a similar clause

While the Student Data Terms are also applicable for Dutch educational institutions, the aforementioned legislation would only be applicable in very specific use cases, namely:

- FERPA (Family Educational Rights and Privacy Act): Applies to US educational institutions that receive federal funding.
- COPPA (Children's Online Privacy Protection Act): COPPA governs the online collection from children under 13 in the US.
- PPRA (Protection of Pupil Rights Amendment): Applies to US educational institutions, regarding surveys or data collection (revealing data such as political beliefs, health, or income) from students.

These laws are applicable only when Dutch educational institutions interact with US institutions, offer services to US children under 13, or collect data from students under these regulations. The applicability and relevance for Dutch educational institutions are highly improbable, especially when using Adobe's products. Adobe explains that COPPA and FERPA language specifically excludes customers located outside US (meaning SURF) as they only apply within the US.

10 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 Adobe applies in its role as data processor and data controller.

10.1 Retention periods Adobe as data processor

The various legal documents include different clauses on retention periods.

Table 17: Comparison provisions on retention periods

Adobe DPA June 2024	Student Data Terms	Adobe General Terms
9.4 "Adobe will, at the choice of the Customer, delete or return to the Customer all Personal Data after the end of the applicable term for Cloud Services, as further specified under the	*7.1"It is the responsibility of Customer to delete or remove Student Data from the Services when it is no longer needed for an educational purpose and/or upon termination of an account or*	*6.5 "With respect to Cloud Services, Customer Data may be permanently deleted from Adobe's servers 25 months from the date of its collection or receipt, unless specified otherwise in the respective PSLT."*

[377] Article 4.1 Adobe Student Data Terms.

Agreement."[378]	*Customer's agreement with Adobe."*[379]	
	7.2 "After termination of an account or Customer's agreement with Adobe, Adobe will retain Student Data for a reasonable period of time[380] *to permit Students to download to and store Student Assets in a personal account. If Customer or Student has not deleted or removed the Student Data through the Adobe Admin Console, Adobe will dispose of or delete Student Data when it is no longer needed for the purpose for which it was obtained*".[381]	*13. "Upon termination or expiration of this Agreement or any License Term for the Products and Services:* *(1) the licenses and associated rights to the Products and Services will immediately terminate;* *(2) …* *(3) Customer Data stored within the Cloud Services will be available to Customer for 30 days after the termination or expiration in the same format then available within the reporting interface(s), unless specified in the respective PSLT"*

The DPA mentions 'all personal data' and the Student Data terms refer to 'student data', while the General Terms that are part of the Enterprise Licensing terms use the term 'customer data'. As described in Section 2.1.2.1 'Personal Data' in Adobe's DPA (June 2024) means 'Customer Data' that relates to an identified or identifiable natural person or as otherwise defined under applicable Data Protection Laws.[382] 'Customer Data' has the meaning set forth in the Agreement.[383]

The General Terms that are part of the Enterprise Licensing terms refer to the PSLT for alternative retention periods. The PSLT for Adobe Desktop Software do not include any relevant clauses. The PSLT for Stock includes a clause on the effect of termination of expiration of the Agreement. The PSLT for Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D determines that *"Adobe will store Customer Content during the License Term up to any storage limit specified in the admin console. Adobe may create reasonable storage limits, such as limits on file size, storage space, and other technical limits. If Customer exceeds those limits,*

[378] 9.4 DPA.

[379] Article 7.1 Adobe Student Data Terms.

[380] Email Adobe: 4 April 2025: "a reasonable period of time is usually determined with the school in question based on their needs following the termination of all of their contracts".

[381] Article 7.2 Student Data Terms.

[382] Article 1.11 Adobe DPA (June 2024).

[383] Article 1.4 DPA Adobe DPA (June 2024).

Adobe will make reasonable efforts to notify Customer to permit transition of Customer Content prior to deletion."[384]

According to Adobe, customers are in control of the retention period of the data passed to Adobe by them as controllers. However, the Admin console does not offer settings to configure retention periods. In addition to this, as described in Section 3.1.5, information is available about how long data is kept after a user is deleted from the user list, but this information is not consistent across the documentation. In addition to the unclear retention period, Privacy Company observed for two accounts that the user's folder remained in the list of *'Active Users'* and was thus retained, even after these two user accounts were removed from the user list. In those cases, the administrator does not have an option to force deletion of the user's folders. The specific retention period for deleted projects is also unclear. The documentation mentions that deleted projects can be restored *"at any time"*, although end-users are told projects are kept for 30 days when removing a project.[385] (see Section 3.1.6).

Adobe Creative Cloud Documents are versioned, and the user can request an overview of older versions from the application. The document can be restored to any of the old versions (see Figure 37). Versions are kept for 180 days, although 60 days is mentioned in some of the application dialogs (this is probably because that was the previous retention period).[386] In case of a *marked* or *named* version, the version is kept indefinitely.[387] Users cannot choose to remove individual versions, it is only possible to remove the whole file including all versions. See also Section 3.2.3.4.

10.2 Retention periods Adobe as data controller

Adobe's privacy policy does not mention specific retention periods. Adobe informs users that:

> *"When you register for an account and create an Adobe ID, we process and keep most personal information we process on your behalf for as long as you are an active user of our Services and Software. We delete certain personal information we collect about you when we no longer have a business reason to retain it. Additionally, there is some personal information we need to retain even after you close your account to comply with business and legal requirements, such as personal information related to our contract and business transactions with you, which we retain for ten years after your last interaction with us.*
>
> *Where we process personal information for marketing purposes or with your consent, we process the information until you ask us to stop and for a short period after this (to allow us to implement your requests). We also keep a permanent record of the fact that you*

[384] Article 9 Storage and Retention, Adobe, PSLT – Adobe Creative Cloud, Adobe Document Cloud, and Adobe Substance 3D (2023v1), URL: https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/PSLT-CreativeCloudandDocumentCloudSubstance3D-WW-2023v1.pdf.

[385] Manage projects, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/projects-in-business-storage.html.

[386] Adobe Creative Cloud enhancements for business plans, last updated 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/enhancements-for-business-plans.html.

[387] Versioning FAQ, last updated 5 April 2022, URL: https://helpx.adobe.com/creative-cloud/help/versioning-faq.html.

> *have asked us not to send you direct marketing or to process your information so that we can respect your request in the future."*[388]

The retention periods in Adobe's legal documentation are not specified. Upon request, Adobe set out details of retention for some of the specific categories of personal data. Both through the response to the DSARs and per email.

Adobe's first response to the DSAR (see also Section 2.4) includes the following information about the retention and data deletion:

> *"Adobe's systems and processes are designed to process your information for only the period that is necessary for the purpose for which it is collected and in compliance with our retention obligations under applicable law, including Dutch law. Now we operate by a system of determining that when data is no longer necessary to retain, Adobe has processes designed to securely destroy and delete such data in accordance with the applicable records retention policy or legal requirements.*
>
> *We have confirmed that when it comes to the Usage and Technical Information this information is generally only kept for 30 days. We have retained it longer in this case given the terms of your request so that we may access it throughout this process (but can delete it when it is complete on your request). When it comes to organizational data, including the personal data in the Profile Information provided, the specific retention period will be controlled by the customer organization for the most part, with only what is necessary retained beyond the customer's active usage period (e.g., after termination).*
>
> *… EDU license admins have broad capabilities to control and delete student data as they see fit and according to their own retention requirements. Adobe would not, as a data processor with limited visibility, be able to determine when a particular student has left school, for instance. In such scenarios, we rely on the local admin users to proactively manage deletion.* [389]

According to this information 'Usage and technical information' would generally only be kept for 30 days. No information is available on 'Profile information'.

In its second response to the DSAR in December 2024 Adobe explains:

> *"while the general rule for centralized logs is that data is retained for 90 days, there are some special cases that can be kept for up to a maximum of 12 months (where necessary in the specific context) while logs related to Adobe Express (ccx-foundation-prod-ew1, ccx-foundation-prod-ue1 and hz_prod) are only kept for 30 days. Product and Services Usage Data is kept for up to a maximum of four years but is deleted sooner than this in many cases."*

The table below lists the retention periods mentioned above.

---

[388] Adobe, Privacy Policy, 'How long does Adobe retain my information?', Last updated: June 18, 2024, URL: https://www.adobe.com/privacy/policy.html.

[389] Adobe DSAR Response from 30 October 2024, p. 12.

Table 18: Retention periods Adobe as controller

Type of data	Retention period
Customer data where Adobe is the controller	for the life of the account plus a maximum cap of four years from the date of the end of the account
Categories of Customer data: Account data, customer contact data and customer profile data	for the life of the account plus 120 days
Logs	90 days. In special cases it can be kept for up to a maximum of 12 months
Usage and technical information	
Customer support data	for up to four years from the date of collection
Financial data related to billing	10 years from the expiry of the contract and for telemetry data in education for four years or the duration of account plus 1 year (whichever is shorter)

Part. B Lawfulness of the 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 Adobe, the processing of special personal data, the application of purpose limitation, the necessity of the processing, and the application of data subjects' rights.

11 Legal grounds

To be permissible under the GDPR, the processing of personal data must be based on one of the legal grounds mentioned in Article 6 (1) GDPR.

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. Adobe is a data processor when it comes to providing the contracted Cloud Services. But in practice, Adobe also processes personal data for its own purposes as data controller. The gap between the contractual and factual reality makes it essential to clarify who determines the purposes and means of the processing. Each purpose must have a valid legal basis, and understanding these roles is necessary for assessing whether the legal bases are properly in place.

11.1 Contractual context and role determination

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 based on factual circumstances. However, the contractual framework can offer guidance on how these roles are carried out in practice.

Creative Cloud and Document Cloud are standard products offered by Adobe, both directly to end users and to enterprise customers. As per Adobe's DPA, the Customer (in this case the educational institution) is the data controller for Customer Data, and Adobe is the processor. The controller determines both the purposes and the means of the processing. However, in this case the purposes outlined in the DPA are formulated too broadly, and the means are not specific enough.

As described in Part A, the DPA does not provide a comprehensive or definitive list of personal data. It mentions Customer Data in the main body of the text and gives examples in Exhibit 1. The data listed includes identification and contact details such as name, date of birth, email address, phone number, title, and physical address; information about individuals' transactions and interactions with the customer's services; and IT-related data, including IP addresses, cookie data, and location information. According to Adobe this is a standard list of the types of data likely to be processed by Adobe solutions.[390]

In addition to the lack of specificity regarding the types of personal data being processed, the purpose of processing is also defined in overly general terms.

[390] Email Adobe 28 March 2025.

> *"Adobe will use, retain, disclose, or otherwise Process Personal Data only on behalf of Customer and for the limited and specific business purposes (as set out in Exhibit 1) of providing the Cloud Services and in accordance with Customer's instructions, including as described in the Agreement."*[391]
>
> *"The purpose of Processing under this DPA is the provision of the Cloud Services pursuant to the Agreement."*[392]

Data processors may only process personal data on behalf of the data controller.[393] Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a data controller in respect of that processing and may be subject to sanction for going beyond the controller's instructions.[394]

The purpose "*provision of the Cloud Services pursuant to the Agreement*" is too broad. Even if the processor offers a service that is preliminarily defined in a specific way (like Adobe's products), the controller must be presented with a detailed description of the service and must make the final decision to actively approve the way the processing is carried out and request changes if necessary. [395] This description allows the controller to ensure that the DPA accurately includes the purposes and the means of the processing and serves as a proper instruction for how the processing should be carried out. If the purposes for processing are too vague, it creates room for interpretation. In such cases, the processor may end up determining additional (compatible) purposes for the processing. By doing so, it would no longer be acting purely as a data processor but would instead take on the role of a data controller.

The current wording in the DPA is so broad that it allows Adobe to perform almost any activity in various roles. The lack of specificity not only makes it difficult to factually establish whether the DPA correctly reflects the roles of controller and processor but also influences the ability to assess the legal basis for processing (and who must have the legal basis for the processing). When Adobe acts as an independent data controller, the education institution must have a valid legal basis for disclosing personal data to Adobe as a third party. Secondly, Adobe must have a legal ground for all the data processing, including 'further' processing for its own purposes. 'Further' processing is only allowed if it is compatible with the initial purposes of the data collection. The compatibility will be assessed in Section 13.

In response to the first draft of Part A of DPIA, Adobe explained that during negotiations (before the agreements were entered into) SURF opted to use the standard DPA, as the previous process was more complex and involved greater difficulties in obtaining signatures from members for SURF's template. [396] In other words, it appears that it was SURF's choice to use Adobe's DPA that

[391] Article 3.4 of the Adobe DPA.

[392] Exhibit 1.

[393] Article 28(3) GDPR.

[394] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, nr. 81, URL: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

[395] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, nr. 30, URL: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

[396] Email Adobe 28 March 2025.

is available online. Each education institution holds individual responsibility. Consequently, if the DPA changes multiple times during the term of the license, not all institutions will necessarily be aligned under the same DPA. This creates a significant administrative burden for SURF to continuously monitor, verify, and follow up with each institution after every DPA update.

In addition to the DPA, other contractual documents also include clauses related to the purposes of the processing. As described in Section 4.1.1 the Enterprise General Terms and the Student Data Terms that form part of the Agreement also include certain permitted (and prohibited) uses of personal data by Adobe. It allows Adobe and its Affiliates to use, copy, transmit, sub-license, aggregate, model, index, store and display Customer Data to perform its obligations under the Agreement. But it also allows Adobe to process Customer Data for Adobe's following own purposes:

- for product improvement and development;
- to publish and distribute any anonymized information (i.e. information where neither Customer nor its site visitors are capable of being identified, which may be aggregated with other customers' anonymous information); or
- to enforce its rights under this Agreement.

For these specified purposes, Adobe acts in the capacity of a data controller and determines the purposes and the means of the processing independently. The legal bases for these processing operations are assessed in Section 11.3

While Adobe's standard DPA creates uncertainty about who the controller and processor are for specific processing activities, other factors also contribute to the ambiguity. SURF's agreement with Adobe (see Section 1.5.2), which states that Adobe is the Consortium Member's data processor, and the Consortium Member is the data controller in connection with the collection of Student personal data *"in the Offering and in another Adobe application that Consortium Member allows K-12 Students to access".* For further details about how Adobe collects, uses, and discloses personal data collected from Students it refers to Adobe's Privacy Policy, which lists Adobe's data processing operations as data controller. Adobe clarified that *"they only point to the Adobe Privacy Policy for "further details"- when it comes to processing as a processor, the Data Processing Agreement together with the General Terms is instructive."* [397]

11.2 Legal grounds for educational institutions

This section assesses the potential legal bases for educational institutions for using Adobe Creative Cloud and Adobe Document Cloud.

The use of Creative Cloud and Document Cloud by schools and universities can be essential for fulfilling their tasks. For example, Creative Cloud may be used to provide education to students and to create educational materials. Document Cloud may be used to support a wide range of public tasks.

When universities use the software to deliver education and use the software for operational or administrative purposes, the processing of personal data can be based on the necessity to perform tasks in the public interest. This legal basis may be applied alongside the necessity of

[397] Email Adobe 28 March 2025.

fulfilling education agreements with students or fulfilling employment contracts and, in certain limited cases, the legitimate interests of the organisations involved.

The organisations will not use the Cloud Services for a vital interest or a legal obligation.

11.2.1 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.[398] Employees and students may not be free to refuse or withdraw consent for the processing of their personal data without facing adverse consequences.

The fact that educational institutions fulfil public tasks are public authorities 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."*[399]

According to the Student Data Terms, Adobe requires educational institutions to obtain parental consent, including verifiable consent from parents or legal guardians, regarding cross-border data transfers. Adobe clarified in its response to Draft A of this DPIA, that consent is the legal bases, *"if required in the applicable jurisdiction. As per our contracts, the Controller would be responsible for the legal basis for this category of data."*

Regardless of the question if consent would be required for any cross-border data transfers, Adobe's requirement for schools to provide parental consent diametrically opposes the definition of 'freely given' consent. If educational institutions want to use Creative Cloud as part of their lessons, they could only include the children whose parents have allowed the processing, stigmatizing and excluding the children whose parents have made different privacy decisions.

---

[398] 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.*"

[399] EDPB, *Guidelines on consent*, paragraph 3.1.1.

11.2.2 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."*[400]

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.[401] 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."*[402] 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.[403] 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."*[404]

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.

11.2.3 Processing is necessary for a task in the public interest

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".*

If schools for example require students to use Creative Cloud as part of the learning curriculum, in principle they can rely on the legal ground of public interest (if the data processing is not unlawful).

---

[400] 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.

[401] ABRvS 20 September 2017, ECLI:NL:RVS:2017:2555.

[402] CJEU 4 July 2023, ECLI: EU:C:2023:537 (Meta vs Bundeskartellamt) paragraph 98.

[403] 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.

[404] CJEU 4 July 2023, ECLI: EU:C:2023:537 (Meta vs Bundeskartellamt) paragraph 99.

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 order to rely on this legal basis, institutions must carry out a necessity test to demonstrate that the processing operations are necessary for the proper performance of their public task.

11.2.4 Necessity for the legitimate interests of the controller or a third party

Processing operations that are not necessary for the performance of a public task may nonetheless be necessary for the pursuit of a legitimate interest of the institution (Article 6(1)(f) GDPR). In order to rely on this legal basis, it must be assessed whether the institution (1) has a legitimate interest, (2) whether the processing is necessary for the pursuit of that interest, and (3) whether the interests of the institution outweigh the interests or fundamental rights and freedoms of the data subjects.

11.3 Legal grounds for Adobe

When acting as a processor, Adobe is instructed by the educational institution and works on behalf of that organisation. The legal grounds for processing used by the organisation then also apply to Adobe as a processor.

As per the Agreement, Adobe is permitted to process Customer Data for their own purposes (and thus the capacity of data controller). If Adobe would process personal data to comply with a legal obligation, they would also do that in the capacity of data controller. In addition to this, several other processing operations were identified in which Adobe processes the personal data for its own purposes, such as the review of content to identify illegal and abusive cloud content and flagged content and storing content credentials.

11.3.1 Consent

According to its Privacy Policy, Adobe relies on consent (Article 6(1)(a) GDPR) as the legal basis for sending marketing communications, using cookies and similar technologies, and accessing certain device information (like location or camera) to enable specific features. Consent is also required for participating in promotional activities such as sweepstakes and contests. Finally, Adobe relies on consent for analysing user behaviour to prevent misuse, improve services, or respond to support requests.[405]

Marketing communications

The organisation's subsegment in the organisation's setting (e.g. K12 and HED) and user roles influence some of the data processing by Adobe. Adobe indicates that they opt-out users of marketing communications if they are marked as students. In all cases, Privacy Company was still able to opt-in to marketing mailing lists but did not receive emails in all cases (see Section 3.2.2.2 for details).

[405] Adobe Privacy Policy, last updated 18 June 2024, URL: https://www.adobe.com/privacy/policy.

Adobe needs to ensure that its consent mechanism for marketing messages meets the legal requirements: only send marketing messages after an active opt-in.

As described in Section 3.2.2.2 Adobe has a system in place that identifies email addresses associated to K12 student users and records them as “opted out” for email marketing communications. As a result, K12 student users are blocked from all non-operational messages sent by Adobe systems.

Cookies

Adobe’s cookie banner presents both strengths and areas for improvement. Users are given the option to enable or not enable cookies on the same layer, without any visual distinction or bias toward either choice. Additionally, the second layer allows for reasonably clear individual cookie preferences, and a link to cookie settings appears to be accessible from most pages.

There are some shortcomings in the cookie details provided on the second level of the cookie banner. Only rudimentary details are offered (cookie name, domain, host, duration, type and category). The exact purpose of the cookie, data stored and third party involved are not described. The stated purposes are in vague and generic terms, lacking specificity and transparency. Statements such as "to improve your experience and measure your interactions..." do not sufficiently explain the extent of data processing. This makes it difficult for data subjects to fully understand what parties the cookies belong to and what the cookies’ functions are, and it affects the users’ ability to make an informed decision whether to consent. Under Article 6(1)(a) GDPR, valid consent must be specific and informed. Without clear information on what data is collected, how it is used, and by whom, the consent given cannot be considered valid under the GDPR. However, the associated risks are reduced by the fact that educational users cannot opt-in for personalised advertising cookies, avoiding the most invasive data processing scenarios.

11.3.2 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 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 Creative Cloud for Education contract is not concluded with the data subject (the individual user), but with the educational institution. Adobe does not rely on this legal basis for any processing of Customer Data.

11.3.3 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:[406]

- 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;

[406] https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en#toc-4

- 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'.

Adobe relies on the legal basis of Article 6(1)(c) GDPR to respond to requests from government or law enforcement agencies during investigations and to use or share data as necessary to detect, prevent, or address fraud, security threats, illegal or deceptive activities, misuse of its services and software, or technical problems such as software piracy.[407]

Adobe commits to redirecting Government and Law Enforcement Inquiries ("Third-Party Demand") to the Customer. If that is not possible, Adobe will, to the extent legally permitted to do so, provide the Customer reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Customer to seek a protective order or other appropriate remedy.[408] These guarantees only apply to the Customer Data, not the other categories of personal data that are processed by Adobe for the provision of the services.

If the legal obligation originates from outside Union law or member state laws, clearly representing a foreign legal obligation, this legal obligation cannot serve as a legal basis for Adobe.

11.3.4 Necessity for the legitimate interests of the controller or a third party

Adobe relies on its legitimate interests for the three permitted uses of Customer Data included in the General Terms:

- Product improvement and development
- Statistics / anonymized information
- To enforce its rights under this Agreement

11.3.4.1 Product improvement and development

Product improvement and development is included in the General Terms without further context. However, Adobe's Privacy Policy lists several sub-purposes, and Adobe may process Customer Data for one or more of these. The sub-purposes include: tracking and analysing user navigation and interaction with the services, analysing user-generated content for product improvement, measuring and improving effectiveness of the software and websites performing content analytics to personalize user experience, using automated techniques and human review to detect technical issues and improve features

Adobe's Content Analyses FAQ states that when users access their account under a business profile or account, then the user has been automatically opted out of content analysis for product improvement.[409] Although the FAQ indicates that content data is not used by Adobe for

[407] Adobe Privacy Policy, 'How does Adobe use the information it collects about you, and what are the legal bases for these uses?', Last updated: June 18, 2024, URL: https://www.adobe.com/privacy/policy.html#how-does-adobe-use-the-information-it-collects-about-you-and-what-are-the-legal-bases-for-these-uses.

[408] Article 9.5 Adobe DPA.

[409] Adobe, 'Content analysis FAQ',
Last updated on Jul 30, 2024 | Also applies to Adobe Creative Cloud, Document Cloud, URL: https://helpx.adobe.com/manage-account/using/machine-learning-faq.html.

product improvement, the term 'Customer Data' is broader than only Content Data and not clearly defined in this context. It is unclear which categories of personal data are included, how they are used for product improvement and development, and whether appropriate limitations and safeguards are in place. While product improvement currently may not be caried out with the use of Content Data, the DPA still allows for the processing of personal data for this purpose. Most probably the data that is used for this processing is 'Product Services Data'.

A legitimate interest is likely present for Adobe. However, there is insufficient information to assess whether the processing is necessary and whether the fundamental rights and freedoms of the data subject are adequately protected.

11.3.4.2 Statistics / anonymized information

According to the General Terms, Adobe is permitted to use Customer Data to publish and distribute any anonymized information (i.e. information where neither Customer nor its site visitors are capable of being identified, which may be aggregated with other customers' anonymous information). This purpose is too broadly formulated. It is unclear which categories of personal data are included, how they are anonymised, and whether appropriate limitations and safeguards are in place.

In response to the full draft of this DPIA, Adobe clarified that any personal data will be anonymised according to EDPB Guidance.[410]

The Student Data Terms include a similar clause about the use of 'de-identified data'. According to Article 6.1 of the Student Data Terms, Adobe may use de-identified data for *"any lawful purpose, including, but not limited to, the development, research, and improvement of educational sites, services, or applications; to demonstrate the effectiveness of the Services; and to inform, influence, or enable marketing, advertising, or other commercial efforts by Adobe."* The Article then states: *"Unless permitted or required by law, Adobe agrees not to attempt to re-identify any such data. Adobe has no obligation to delete de-identified data."*

It is not clear in what context Adobe would be permitted or required by law to attempt to reidentify any such data. Besides, the fact that the data apparently can be re-identified explains that the data are pseudonymous data (not anonymous) and, thus, still qualify as personal data.

A legitimate interest is likely present for Adobe. It depends on the aggregation and anonymization if it would meet the necessity requirement. It is concerning that the Student Data Terms that are applicable in the current contractual framework in which Adobe claims to have no obligation to delete de-identified data, especially as the clause in these Terms leaves open the possibility of re-identifying the data.

In response to the full draft of this DPIA, Adobe explained that the term 'de-identified data' *"comes from the commonly accepted definition […] used by the U.S. Federal Trade Commission and U.S. state laws such as the California Consumer Privacy Act, all of which require that companies publicly commit not to "attempt to re-identify" de-identified data. That statement does not mean that data can always be re-identified. Moreover, the section seems to misunderstand the overlap with the Student Data Terms discussion of use of de-identified data.*

[410] Adobe response to SURF additional questions 8 August 2025 (17 Oct 2025).

As set forth in the terms, de- identified data is data that has not been re-identified and as such should be available for the same uses as non-personal data."[411]

11.3.4.3 To enforce its rights under this Agreement

Adobe is also permitted to use Customer Data to enforce its rights under the Agreement. Again, it is unclear what data is involved, how it will be processed, or under what procedures. Enforcing rights could encompass a wide range of actions, from litigation and debt collection. Adobe would rely on its legitimate interests for this purpose.

It is Adobe's legitimate interest to protect its interests. "Enforce its rights" can be interpreted widely and potentially can influence data subject's rights. The broad phrasing of this purpose leaves too much room for interpretation and does not sufficiently safeguard the rights and freedoms of the data subjects.

In addition to the three purposes permitted in the General Terms, it also is apparent that Adobe processes Customer Data for the next purposes:

11.3.4.4 General communication to users

Adobe processes Customer Data to send general communications to parents, legal guardians, school employees or Adobe customer accounts (associated with the licenses) only about their existing entitled services, *"not first-party advertising or efforts to upsell additional products*". For example, these are notifications to parents about their own access to Creative Cloud if an institution enables it as part of a student's entitled services or informing students about updates to their login process, such as when their institution adopts a new identity provider on student devices that may alter or provide new options for logging into their entitled Adobe services. Adobe relies on its legitimate interest for such activities, and this processing most probably would pass the balancing test.

If those messages or emails contain web beacons or pixels, the e-Privacy Directive is applicable. In addition, to the use of web beacons in Adobe's service messages Article 11.7a(3)(b) of the Dutch Telecommunications Act (hereinafter: Tw) applies. In response to the full draft of this DPIA, Adobe explained that the data collected via the web beacons in the operational emails is limited. *"For "opening" data it is limited to the timestamp (e.g., specific time) that an email was opened together with any potential URL click (e.g., if confirming user login was legitimate). There is no personal data such as IP Address or User Agent details being collected by either tracker."*[412]

The Dutch Telecommunications Act allows an exception for cookies or similar technologies when they are used solely to measure the quality or effectiveness of a service and have no or only minimal impact on user privacy. Web beacons fall under this exception when they process only limited data and do not meaningfully affect the user's private life. In this case, the beacons are included only in service-related emails (not for commercial or marketing purposes) and the data is limited (as per Adobe) so the privacy implications are minor. Given the limited impact this purely analytical tool has on the privacy of the aforementioned individuals, no consent under the Dutch Telecommunications Act is required.

[411] Feedback 18 December 2025.

[412] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025.

11.3.4.5 Creation and storage of content credentials

Adobe's processing of Content Credentials is based on legitimate interest. Adobe explained:

"The interests pursued are lawful and Adobe's purpose is to promote transparency around the use of generative AI (i.e., to address the prevalence of misleading information online by verifiably recording the provenance of any digital media, including content made with generative AI).

Content Credentials complement the existing legal framework, in particular Art. 50(2) of the AI Act, which requires providers of AI systems generating synthetic audio, image, video or text content to ensure that the outputs are marked in a machine-readable format and detectable as artificially generated or manipulated. Content Credentials, which are human-readable, provide an additional layer of transparency, on top of what is mandatory.

Content Credentials also include technical data (output thumbnail, issuer, date, app or device used, AI tool used and actions) and global user IDs (GUID). Users may, at their option, provide further information (e.g., names, social media accounts). Unlike other data items, GUID are accessible only to Adobe, not to the public. So, the personal data within Content Credentials are limited in scope, innocuous [harmless] in nature, and not entirely public. It is therefore very unlikely that the processing of such data will adversely affect users.

Content Credentials are an industry-standard metadata type. They are being implemented not just by Adobe, but also by leading organisations around the world. Their wide recognition allows users to reasonably expect that any content they provide or disseminate through a service may be subject to the provider's voluntary own-initiative investigations into illegal content. Adobe strengthens these expectations by providing a transparency page.

The processing benefits data subjects themselves, as well as third parties. In our legitimate interest analysis we also included an assessment regarding data subjects. Content Credentials can help them receive recognition for their content as it is published and shared online. In that context, Content Credentials contribute to protecting authors' moral rights (Art. 6b is of the Berne Convention for the Protection of Literary and Artistic Works), i.e., "the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation".

Also, with regard to third parties, Content Credentials provide a trusted, transparent way for consumers and media to distinguish between what is actually owned or created by brands, organisations and users and what is being duplicated, replicated, or even faked. In that context, Content Credentials contribute to protecting freedom of expression and information as enshrined in the EU Charter of Fundamental Rights."[413]

11.3.4.6 Detection and review of illegal content

Adobe employs both automated techniques and human review to analyse user content stored Adobe analyses the user's content and its characteristics using automated techniques or with human review, in case of illegal and abusive cloud content, and public and shared cloud content. *"Cloud Content may be automatically scanned to ensure we are not hosting illegal or abusive content, like Child Sexual Abuse Material. Human review may occur when your Cloud Content is*

[413] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025.

flagged or reported as illegal or abusive". All public and shared Cloud Content is subject to review for intellectual property issues and safety issues (for example, violence and nudity). This also applies to business and education organisations.[414]

Proactive scanning for CSAM by cloud service providers currently lacks a direct legal requirement under either EU law or United States law. In the United States, 18 U.S.C. § 2258A requires providers to report known CSAM to the NCMEC but does not impose an obligation to proactively detect such material. Scanning of user-hosted content, including the use of hashing and machine learning (collecting personal data in order to prevent and detect criminal offences), is therefore conducted voluntarily by Adobe and is not required by law.

The DSA acknowledges that providers of intermediary services may "in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content" (Article 7 DSA). The DSA cites "images depicting child sexual abuse" as illegal content (Recital 12).

According to Adobe, its *"interest in combating child sexual abuse is legitimate; it is consistent with existing EU legislation, including Directive 2011/93 (minimum rules on definition of criminal offences and sanctions in area of sexual abuse/exploitation of children and child pornography) and – in the electronic communication sector – Regulation 2021/1232 (temporary derogation from the ePrivacy directive for processing to combat child sexual abuse)."*[415]

In cases where content is flagged or reported as potentially illegal or abusive, it is subject to further human review to ensure compliance with legal obligations and platform safety standards. All content that is shared or made publicly accessible through Adobes Software and Services is subject to additional scrutiny. Automated systems may review such content for issues related to intellectual property rights and user safety, including but not limited to violence, nudity, spam, and phishing attempts. When users make their Cloud Content publicly available, Adobe may initiate human review processes to assess potential violations and maintain platform integrity. According to its Privacy Policy, Adobe relies on the legal basis of legitimate interests (article 6 (1) (f) GDPR) to carry out this processing.

11.3.4.7 Reporting illegal content

All confirmed matches are reported without further balancing test. There are no exceptions to the reporting to NCMEC. NCMEC sends aggregated feedback and statistics on the quality of reports. These reports are not publicly available but confidential. Adobe has been highly rated in comparison to other software providers.

In Meta vs. Bundeskartellamt the CJEU ruled "*that, in principle, collecting and sharing personal data with law enforcement authorities in order to prevent, detect and prosecute criminal offences is not an objective that is capable of constituting a legitimate interest pursued by a private business operator whose activity is essentially economic and commercial in nature. Therefore, such an operator would generally be unable to rely on such a legitimate interest,*

[414] Email Adobe 13 December 2025.

[415] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025.

which is unrelated to its economic and commercial activity, to process personal data for that purpose on the basis of Article 6(1)(f) GDPR".[416]

In response to the full draft of this DPIA, Adobe explained it does not collect and store personal data specifically to be able to provide such data to law enforcement agencies. It does so primarily to enforce its policies and commitments to child safety (including to terminate any user account found to have uploaded or created CSAM). *"Voluntary disclosure to law enforcement agencies is secondary to that process and as such is validly underpinned by Adobe's legitimate interest."*[417] Adobe relies on its legitimate interests for the reports to NCMEC but does not perform individual balancing tests. Adobe did not confirm any process involving Dutch law enforcement. Adobe stated: *"NCMEC is uniquely situated to rapidly and credibly report instances of ongoing abuse to local law enforcement on an emergency basis, which is why Adobe follows the industry standard of making reports to NCMEC allowing NCMEC to use its unique expertise and knowledge to address emergency situations in the best way possible".*[418]

12 Special category data

Special categories of data are *"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"* (Article 9 (1) GDPR).

With special categories of data, the principle is one of prohibition: these data may not be processed. The law contains specific exceptions to this rule (which must be interpreted strictly)[419], for instance when the data subject has explicitly consented to the processing for one or more specified purposes (Article 9 (2) (a) GDPR), or when personal data have been 'manifestly made public by the data subject' (Article 9 (2) (e) GDPR).

The data protection risks for data subjects are not limited to the processing of special categories of data. Similar risks may apply to other categories of personal data of a sensitive nature, classified or secret data. The EDPS explains in its guidelines on the use of cloud computing services by European institutions that special categories of data should be interpreted broadly when interpreting the risks for data subjects. The EDPS writes: "*Nevertheless, this is not the only factor determining the level of risk. Personal data that do not fall under the mentioned categories might lead to high levels of risk for the rights and freedoms of natural persons under certain circumstances, in particular when the processing operation includes the scoring or evaluation of individuals with an impact on their life such as in a work or financial context, automated decision making with legal effect, or systematic monitoring, e.g. through CCTV.*"[420]

---

[416] Idem, nr. 31 and See CJEU, judgment of 4 July 2023, Case C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), para. 124 and 132.

[417] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025.

[418] Feedback Adobe 18 December 2025.

[419] CJEU 4 July 2023, ECLI: EU:C:2023:537 (Meta vs Bundeskartellamt) paragraph 76. And see, to that effect, judgments of 17 September 2014, Baltic Agro, C 3/13, EU:C:2014:2227, paragraph 24 and the case-law cited, and of 6 June 2019, Weil, C 361/18, EU:C:2019:473, paragraph 43 and the case-law cited

[420] EDPS, Guidelines on the use of cloud computing services by the European institutions and bodies, 10 March 2018, URL: https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf.

The EDPS also refers to the criteria provided by the Article 29 Working Party when a Data Protection Impact Assessment (DPIA) is required.[421]

There are many possible scenarios where universities might use Adobe's Creative Cloud or Document Cloud to process special category data. The assessment of the lawfulness of these processing operations is out of scope of this DPIA.

Article 6 (3) (c) of the General Terms[422] reads:

> *"Unless specifically agreed to by Adobe in writing, Customer agrees not to collect, process, or store any Sensitive Personal Data[423] using the Cloud Services or otherwise make Sensitive Personal Data available to Adobe or Adobe's third-party providers."*

While the clause serves as legal protection for Adobe, it overlooks the practical reality of how the different software (especially Document Cloud) is typically used by organisations. Adobe can process several types of special category data through user generation content.

When acting as a processor, Adobe is instructed by the educational institution and works on behalf of that organisation. The legal grounds for processing used by the organisation, including any applicable exceptions for processing special category data, also apply to Adobe as a processor.

The legal exceptions for the processing of special category data for Adobe when acting as a data controller are described below.

13 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*

[421] Article 29 Working Party (now: EDPB), WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, URL: http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236.

[422] Adobe General Terms (2024v1), (2024v1), Effective Date: 8 March 2024, URL:

https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/GeneralTerms-NA-2024v1.pdf.

[423] "Sensitive Personal Data" means an individual's financial information, sexual preferences, medical or health information protected under any health data protection laws, biometric data (for purposes of uniquely identifying an individual), personal information of children protected under any child protection laws (such as the personal information defined under the US Children's Online Privacy Protection Act ("COPPA")), and any additional types of information included within this term or any similar term (such as "sensitive personal information" or "special categories of personal information"), as used in applicable data protection or privacy laws (Article 1.31 General Terms)..

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."[424]

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'."*[425]

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).

Adobe and the educational institutions cannot be qualified as joint controllers; therefore Adobe must be qualified as third party to which the education institution and disclose personal data. This disclosure is a form of 'further processing' in relation to the purposes for which the universities and the plan to use the Cloud Services.

Exhibit 1 describes the purpose of the processing as *"the provision of the Cloud Services pursuant to the Agreement."* This description of the purpose lacks the specificity and clarity required under Article 28 (3) GDPR. It is non-limitative and does not explicitly describe the processing activities and instead refers to a separate agreement, making it unclear where the actual purpose is defined.

To assess the legitimacy of this further processing for different purposes (Adobe'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.

The purposes are articulated so broadly that they can over a wide range of activities. The purpose is not specific, nor limited to specific personal data. Absent any contractual limitations,

[424] 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.

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

Adobe could process the Customer Data it processes because of the use of Creative Cloud and Document Cloud for various purposes.

14 Necessity and proportionality

14.1 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.

14.2 Assessment of the 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.

14.2.1 Lawfulness, Fairness, and Transparency

Data must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject' (Article 5 (1) (a) GDPR). This means that data subjects must be informed about the processing of their data, that all the legal conditions for data processing are adhered to, and that the principle of proportionality is respected.

Adobe states it uses both fingerprinting techniques and machine learning to detect CSAM. Adobe does not provide any details on the machine learning, models used and its training set.

Lawfulness

Besides the unclear roles and processing purposes in the Agreement, the contractual structure has other gaps. Hierarchy clauses are missing, and not all relevant documents properly reference each other. For example, both Adobe's DPA and the Student Data Terms apply to SURF's Agreement and no hierarchy between them is defined. In addition to this, Adobe's Enterprise Licensing Terms, its General Terms, and Specific Product Licensing Terms are not mentioned in

the Student Data Terms. This potentially influences the lawfulness of the processing and at least causes a loss of control.

About the locations of processing of personal data for Firefly, Adobe states: *"Adobe currently processes, caches and potentially stores Firefly input content in Amazon Web Services (AWS) data centers in the US-East and US-West, regardless of the user's location. Adobe Firefly stores Generation History in Enterprise Storage in the US-East, EMEA-West, and APAC-East regions. Adobe currently stores Content Credentials in AWS data centers in the US-East region, regardless of the user's location. If applicable, Adobe currently stores indemnification data in a licensing database hosted in the EMEA-West region, regardless of customer location."*[426] It is unclear what data is stored in the US and what data processing activities are performed in the US. It is also not specified for what purposes this data is processed in the US. It is therefore difficult to assess the lawfulness.

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.[427] There are several circumstances that might be unexpected for the data subject.

When an end-user creates a project, the fact that administrators can see the name of the created project is not mentioned directly, only in the documentation pages.[428] Users typically assume that their personal or project-related information is kept private unless explicitly shared. Without proper awareness, data subjects are not able to make informed decisions. They might choose a different name for the project.

When administrators give other users (or themselves) access to a project, the original project creator is not notified of this change in access to the project. The lack of notification about changes in access undermines the creator's control and expectation of privacy over their work.

Users cannot easily see which Creative Cloud files they have shared: the Creative Cloud web application does contain a *'Shared with'* column in its list view, but that only contains information (the number of contributors) if the file has been shared with individual contributors. If a file was shared with the whole organisation or anyone (or if it is a Document Cloud file), the column is empty. Adobe has confirmed they are working on improvements in this area.[429]

Several features in Acrobat and Photoshop connect to the Adobe Cloud to perform actions. Sometimes the user has an option to disable the online functionality or choose between a local or online implementation. In other cases, the user is not directly aware that the functionality is offered by an online service. An example of the latter is the Firefly AI functionality discussed in Section 8.1, which cannot be disabled by the end-user.

---

[426] Adobe: Security fact sheet, Adobe Firefly for enterprise, Core and Web, March 2025, URL: https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

[427] 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.

[428] Creative Cloud projects overview, last updated: 30 December 2024, URL: https://helpx.adobe.com/sg/creative-cloud/help/projects-overview.html.

[429] Email Adobe to SURF, 28 March 2025: *"We are aware of this, and investigations are underway to incorporate the capability to show when the document is shared in all cases in the referred list view. "*

During testing, Privacy Company noticed that administrators can access Creative Cloud files (Photoshop and Adobe Express) if they know the unique identifier which is used in sharing URLs (also see Section 3.2.3.2). This is also somewhat documented in the collaboration FAQ: *"When you attempt to share an asset with an administrator, you will see the message Administrators already have access."*[430] As these unique file identifiers are present in the content logs (see Section 3.1.11), administrators are able to access files without user intervention and without the user being aware of this, even though the security whitepaper claims otherwise. This method does not work for Document Cloud (Acrobat) files. It would be unfair for administrators to access the files without the user's knowledge as the user would not expect this and is not made aware of it.

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).

Adobes Cookie Statement aims to give context on the cookies and technologies used, but fails to provide a comprehensive list of cookies, technologies, and their retention periods. 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."[431] 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) phrase 1 GDPR and may only be used if controllers are able to demonstrate that this does not undermine the fairness of processing.

Adobe's cookie banner does present individual cookie details and a link to cookie settings appears to be accessible from most pages. However, only rudimentary details are offered (cookie name, domain, host, duration, type and category). The exact purpose of the cookie, data stored and third party involved are not described. Like the cookie statement, the banner states purposes in vague and generic terms, lacking specificity and transparency.

The list of third-party sub-processors was also not complete at the time of writing this DPIA. The list does mention Akamai, Cloudflare and Fastly, but it did not specify that they are used for the services assessed in this DPIA, while traffic to these service providers were observed. Adobe has updated the subprocessor list as of December 2025 to address this issue. It does seem that the 'Description' column was not (fully) updated. E.g., for Cloudflare it states "Adobe does not route user information through Cloudflare" but in reality, Adobe's main authentication page (auth.services.adobe.com) is routed through Cloudflare and thus processes user credentials. For Fastly the description only mentions Adobe Experience Cloud. So, while there are improvements made in this area, the descriptions still need to be completed to lower the probability of the risk occurring.

[430] Collaboration FAQ, last updated: 6 October 2023, URL: https://helpx.adobe.com/creative-cloud/help/collaboration-faq.html.

[431] EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces, par. 74.

14.2.2 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). This means that the controller may not collect and store data that are not directly related to a legitimate purpose. According to this principle, the default settings for the data collection should be set in such a way as to minimize data collection by using the most privacy friendly settings.

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.[432]

As part of their products, Adobe collects telemetry on product usage (see Section 2.3.1.1). Adobe also returned (part) of this telemetry data in the DSAR responses (see Section 2.4). As part of their Usage Data FAQ, Adobe states that for business profiles they do not receive 'desktop app usage data' but do collect 'operational and license information'.[433]

The telemetry data as observed in the network traffic and seen in the DSAR responses seemed to contain high-level information on the user navigating through the Adobe applications. This data collection does not seem to be in line with Adobe's statement that 'desktop app usage data' is not collected for business profiles, unless Adobe considers this data 'operational and license information'.

Further explanation on why the telemetry data is collected is needed to adhere to the principles of data minimisation and privacy by design, as the collected data does not seem to be essential for the operation of the services and thus collection of this data could be excessive.

14.2.3 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).

Administrators and users are generally able to update their personal data when needed (e.g., their name, email or document contents).

In sum, Adobe's data processing respects the principle of accuracy to the extent that it is relevant for this DPIA.

14.2.4 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*

[432] CJEU 4 October 2024, C-446/21 (Schrems vs Meta), par. 65.

[433] Usage Data FAQ: Creative Cloud and Document Cloud Apps, URL: https://www.adobe.com/privacy/app-usage-info-faq.html, last updated: 18 June 2024.

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).

When removing a user from the Admin Console, administrators should be aware that this action alone does not fully delete the user's details from the Adobe organisation. To complete the removal, the user must also be deleted from the underlying directory, either manually or through an automated synchronisation method. The Admin Console does not clearly indicate that user information is stored in multiple locations, making it unclear when a user is truly deleted. Even after full removal, the user's assets may still be retained. As a result, personal data may be kept longer than necessary.

A similar issue arises when Enterprise or Federate ID type users have multiple organisation memberships. For these cases, fully removing an Enterprise or Federated ID requires the administrators to delete the user from three places: the user list, the Business ID directory, and the domain directory.

Adobe's documentation fails to clearly state that user data remains stored even after account removal, unless the administrator manually deletes it. Data of removed users is kept indefinitely, and only deleted 14 days after an administrator removes the user data from the 'Inactive Users' tab in the admin console.[434] This is not apparent from the documentation and inconsistency in the available documentation (see Section 3.1.5.4) makes the actual retention period unclear. Without manual removal and a clear understanding of the retention periods, the user data may be processed longer than necessary. In addition to the unclear retention period, Privacy Company observed for two accounts that the user's folder remained in the list of *'Active Users'* and was thus retained, even after these two user accounts were removed from the user list. In those cases, the administrator does not have an option to force deletion of the user's folders.

Adobe has stated they are working in improvements in this area which are discussed in more detail in Section 16.2.17.[435]

The specific retention period for deleted projects is unclear. The documentation mentions that deleted projects can be restored *"at any time"*, although end-users are told projects are kept for 30 days when removing a project.[436] Adobe clarified that: *"Deleted Projects can be restored within 30 days from the date of deletion. The retention period for Projects is the same as for any other content or asset in ESM, where the content persists until Administrators either reassign them to another or completely delete them from our systems."*[437] Thirty days after testing, Privacy Company no longer observed deleted projects in the admin console. Given these answers, it is still unclear if projects are permanently deleted 30 days after removal by a user, or

[434] Email Adobe to SURF, 28 March 2025.

[435] Response to SURF Concerning Technical Mitigations (31 October 2025).

[436] Manage projects, last updated: 16 December 2024, URL: https://helpx.adobe.com/enterprise/using/projects-in-business-storage.html.

[437] Email Adobe to SURF, 28 March 2025.

persist until an administrator deleted them. If the latter is true, personal data may be processed longer than necessary.

In addition to the issues administrators face with user and data deletion, users can also be restricted in their ability to delete documents. For example, creating a project library with *restricted* permissions leads to problems when the creating user chooses to *'Leave'* the library (which is the only option the Creative Cloud web application offers for such libraries, as the *'Delete'* option is only available in the desktop interface, see Figure 36). In these cases, their own permissions are removed, and they are no longer able to remove the library or files in that library. This can lead to a situation where none of the users in the organisation is able to remove the files from the library and the only option is to delete the whole project containing the library.

Furthermore, content credentials are retained indefinitely, despite the unclear purpose (See Section 8.1.5). Adobe includes the global user id (GUID) in the content credentials when generating and storing them. The indefinite retention seems disproportionate, especially considering that even IP laws have defined retention periods.

14.2.5 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).

Content Credentials Inspector

Content credentials can be verified in the 'Content Credentials Inspector'.[438] It is possible to upload an image to the inspector. If the image contains Content Credentials in the metadata, the inspector reads those and verifies the fingerprints. Additionally, the inspector provides the option to search for possible matches to the picture. During testing, some search attempts returned possible matches. The results included other versions of the image that had been created using slightly different prompts during the same testing process. These images had only been downloaded and were never published. Notably, the matches still appeared even when the search was conducted from a browser without cookies or an active login session.

This means that anyone can find and see unpublished versions of an image. Adobe confirmed this is expected behaviour for fully AI-generated content:[439]

> *"Adobe automatically applies a Content Credential to AI-generated content created using Adobe products and services. The credential is applied when the image is generated. After a credential is applied to the image, it is added to the Content Credential public cloud, which is why when you used the inspect tool, the results included an image that was AI-generated and was a near exact match for your search."*

Adobe has also stated this is not expected behaviour for partially AI-generated content.[440]

If images that were never published can still be retrieved through reverse image search, this suggests that user-generated content may be indexed or stored in a way that is potentially

[438] Adobe: Content Credentials Inspector, February 2025, URL: https://contentauthenticity.adobe.com/inspect

[439] Email Adobe to SURF, 28 March 2025.

[440] Email Adobe to SURF, 31 October 2025.

accessible by individuals who were never intended to see it, undermining users' expectations of privacy.

14.3 Assessment of the subsidiarity

The key question is whether the same goals can be reached with less intrusive means.

Educational institutions have the option to have a contract with Adobe that gives universities more flexibility on what applications to use, and whether or not to provide cloud storage in Adobe Creative Cloud. Educational institutions have the option to procure products that let users use single applications instead of all applications, or products that do not allow storage in the Adobe' cloud storage. As discussed in Section 3.1.3, under the current contract with Adobe administrators have the option of disabling some services. Since August 2025, this includes disabling cloud storage for existing contracts (the functionality of this new option was not verified by Privacy Company).

Universities also have the alternative option of distributing managed packages of Adobe products (see Section 3.1.4). Managed packages provide universities a bit more control over some privacy options (for example disabling file syncing). Outside of alternative contracts between SURF and Adobe, commercial and non-commercial alternatives exist for Photoshop, Express and Acrobat. However, part of the reason institutions provide this software to students is the large userbase of this software in various industries. Providing a less widespread but functionally equivalent option to students does not equivalently prepare them for industries where knowledge of Creative Cloud is expected.

Image generation with Adobe Firefly (section 2.3.1.2) has competitors in the market, but due to the nature of generative AI many of the same privacy risks are likely to remain.

In sum: Educational institutions have the option to choose a contract with Adobe that is less intrusive to the rights and freedoms of data subjects, in particular if the contract disables the storage of data in Adobe's cloud storage. Educational institutions may also be able to disable cloud storage within the existing contract.

15 Data Subject Rights

The GDPR grants data subjects the right to information, access, rectification and erasure, object to profiling, data portability and file a complaint. It is the data controller's obligation to provide information and to duly and timely address these requests. If the data controller has engaged a data processor, the GDPR requires the DPA to include that the data processor will assist the data controller in complying with data subject rights requests. This chapter assesses whether educational institutions and Adobe meet the GDPR requirements relating to data subjects' rights and whether data subjects can effectively exercise such rights.

Adobe's DPA includes the following clause:

> *"Adobe will promptly notify Customer if Adobe receives a request from a Data Subject relating to Customer's use of the Cloud Services, including where the Data Subject seeks to exercise any of its rights under applicable Data Protection Laws (collectively, "Data Subject Request"). The Cloud Services provide Customer with controls that*

Customer may use to assist it in responding to Data Subject Requests. Customer will be responsible for responding to any such Data Subject Requests. To the extent Customer is unable to access the relevant Personal Data within the Cloud Services, upon Customer's written request, Adobe will provide commercially reasonable cooperation to assist Customer in responding to a Data Subject Request."[441]

15.1 Right to information (transparency)

Data subjects have a right to information (Articles 12-14 GDPR). 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.

The educational institutions are currently not in a position to effectively inform the data subjects about the processing, as the information provided to them lacks sufficient clarity and is incomplete (e.g. sub-processor list is incomplete). Additionally, Adobe acts as a controller for certain processing activities while this role division is not clear to the data subject. As a result, it is unclear to users who determines the purposes and means of the processing.

15.2 Right to access

Data subjects have a fundamental right to access personal data concerning them (Article 15 GDPR). 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.

The overall aim of the right of access is to provide data subjects with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data.[442] The right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subject's request.[443]

As described in Section 2.4, Adobe has responded to two data subject access requests from Privacy Company. In response to these access requests, Adobe has provided various documents with profile information, service information and application log files. Application log files were not provided for all applications, but it is not known if Adobe had other logs available. Adobe also did not provide any personal data processed by third parties as Adobe's processor, although several of such parties exist (e.g., see Adobe's explanations in Section 5.3.1.2). The response also included codes that are internal to Adobe for audience segmentation, without an explanation to the data subject as to their meaning (see Section 2.4.3.5). Additionally, part of the telemetry data seems to be missing from the responses (see Section 2.4.3.4).

---

[441] Article 9.1 Adobe DPA.

[442] EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 2.0, Adopted on 28 March 2023, p. 3, URL: https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf.

[443] Idem, p. 5.

According to Adobe, Adobe provided all available and responsive application logs for the applications that were in scope for the DPIA. “Regarding telemetry data, Adobe provided all telemetry data collected for product improvement purposes for the applications that were in scope. For Adobe Express, there was no telemetry data for product improvement collected for the user IDs of the accounts used for testing. This may be because users in the Netherlands are automatically opted out of non-essential cookies, and the accounts used for testing did not opt in.” [444]

As discussed in 3.1.5.2, In some cases, administrators (as controllers) may need to access files of end-users (for instance, when a user or legal guardian performs a DSAR). Privacy Company has not identified features provided by Adobe to accommodate such scenarios. Adobe suggested that administrators can access documents of end-users directly (which is not the case for Document Cloud documents, and cumbersome for Creative Cloud documents as knowledge of the document identifiers are required). Another suggestion was to use the remove the user account and use the asset reclamation feature, or to force a change of the user’s password. Both options seem rather drastic ways to adhere to a data subject access request.

In sum, Adobe’s process for providing a right to access is missing relevant tooling for controllers. Adobe has updated information and is making improvements in the tooling. Due to these shortcomings, it will not always be possible to adhere to the right of access of data subjects.

15.3 Right to object

Data subjects have the right to object to processing based on legitimate interests or public tasks, as well as direct marketing (article 21 GDPR). Adobe’s Privacy Policy confirms that when processing is based on legitimate interests, users can object “in certain cases”. If they do, Adobe will stop processing unless it can demonstrate compelling legitimate grounds or a legal obligation to continue. To exercise the right to object, users must know that the processing is taking place. Students or employees may not be aware that Adobe processes personal data for its own purposes, which limits their ability to object.

15.4 Right to rectification and erasure

Data subjects have the right to have incorrect or outdated information corrected, to have incomplete information completed (Article 16 GDPR), and under certain circumstances to have personal data deleted (Article 17 GDPR).

As described in Section 3.1.5.3, Adobe has implemented a deletion process for fully removing a user and the user’s assets. However, there are scenarios where administrators do not have the option to delete user folders, even after users have been removed from the user list, possibly due to bugs in the software. Also, administrators must be aware that user folders need to be manually removed after the user account has been removed. If this is not done, user data will be kept indefinitely, and this is not always clear from the documentation.

As described in 3.1.2.3, Adobe’s documentation contains conflicting information about the process of permanently deleting or reclaiming data and digital assets.

[444] Feedback Adobe 18 December 2025.

In sum, Adobe's documentation and processes for deletion allow for complete deletion of user information and assets (except for limited circumstances that seem to be related to minor software bugs). At the same time, processes can be confusing for administrators due to the number of steps that have to be takes. It is therefore recommended that Adobe reviews their deletion processes to resolve software bugs and clarify documentation, so data subject rights can be fully honoured.

Part C. Discussion and Assessment of the Risks

This section describes and assesses the risks to the rights and freedoms of data subjects resulting from the processing of personal data in Adobe Creative Cloud and Adobe Document Cloud, specifically in the context of an implementation by educational institutions within Adobe's contractual framework established by SURF.

Section 16 provides a general introduction to the method of the risk assessment. Section 16.1 presents context and background on (some of the) risks identified in Section 16.2, which are subsequently mapped in the matrix in Section 0.

16 Risks

Risks to the rights and freedoms of the data subject ('privacy risks') occur when processing activities of personal data violate a right or freedom given to the data subject by the GDPR or any other legislation.

SURF assessed each risk by combining its likelihood with its potential impact on data subjects' rights and freedoms based on SURF's findings in Part A and SURF's legal assessment in Part B of this DPIA. The likelihood refers to the probability that a specific risk will materialise. In other words, how realistic it is that the identified negative consequences for data subjects will occur in practice. High risks usually occur when a processing violates a legal protection of one of the fundamental rights as described in the European Charter of Fundamental Rights, but violations of other rights given by Union or Member State law may also constitute a privacy risk. The impact, or seriousness of the consequences, refers to the severity of the potential harm, taking into account the nature and the extent of that potential harm, the sensitivity of the personal data involved (e.g. special category data, location data), and whether the data subjects are particularly vulnerable (e.g. children). These factors help determine the level of impact.

Any risk that involves a violation of one or more of the GDPR's core principles (Article 5 GDPR) or limits the exercise of the data subject's rights (Chapter III, Articles 12–23 GDPR) in any way, is likely to be categorised as high impact, as it directly undermines the fundamental rights and freedoms. The likelihood and impact are mapped onto a matrix using the ICO model[445] to classify the risk as high or low (See Table 19).

16.1 Context and background of the identified risks

This DPIA identifies several risks relating to the contractual framework and the specific clauses contained within the agreements. It is important to emphasize that these findings are limited to SURF's contracts and do not necessarily reflect a broader issue affecting Adobe in general. The contracts in question were negotiated between SURF and Adobe, and some of the points now highlighted stem from SURF's preferences at the time of negotiation (2022). Adobe noted that some of the clarifications, changes now proposed were not incorporated at that time due those negotiation outcomes. The purpose of this umbrella DPIA is to identify risks and recommend

[445] The ICO model refers to the risk assessment framework developed by the UK Information Commissioner's Office (ICO) to help organisations evaluate risks to data subjects' rights and freedoms in the context of data processing. This is a commonly used framework for conducting DPIAs.

measures to mitigate them. Assessing the contracts forms part of this process. While some of the identified risks are contractual risks, they can still give rise to data protection risks if not addressed. As SURF and Adobe are currently in the process of renewing these agreements, this presents an ideal opportunity to address and correct the identified concerns.

The GDPR (as set out in Recital 1) focuses on the right to the protection of personal data. Data protection harms are complex, wide-ranging and often overlap. While Adobe notes that 'loss of control' is not defined in the GDPR and appears only once in Recital 85, the concept is recognised in regulatory guidance. In particular, the ICO's Data Protection Harms Taxonomy identifies 'loss of control of personal data' as a specific harm category characterised by *"thwarted expectations arising from the misuse, repurposing, unwanted retention or continued use and sharing of personal data, as well as a lack of transparency or commitment to data accuracy"*.[446]

In response to the full draft of this DPIA, Adobe has characterized certain identified risks as product feature requests rather than compliance gaps.[447] However, lacking features that restrict data subjects from deleting or unsharing documents, limit an administrator's ability to fully honour DSARs, or obscure the steps required to properly complete an erasure request, could directly affect the rights and freedoms of data subjects. Regardless of being framed as a 'feature request', these limitations could constitute real risks under data protection law and therefore must be flagged in a DPIA. The purpose of highlighting these risks is to raise awareness for the educational institutions so they can take steps to ensure compliance (where possible). The DPIA also suggests mitigating measures for Adobe to reduce the probability and the impact of these risks. Adobe appears to interpret this as an attempt to shift responsibility from the controller to Adobe, but that is not the intention. The objective is simply to ensure that educational institutions are able to use Adobe's products (in scope of this DPIA) in a compliant manner, with a clear understanding of the risks and the measures required to address them.

Throughout the DPIA process and since the full draft of the report was shared, Adobe assessed the feasibility of the requested technical mitigations and identified which measures it will implement, along with expected timelines. The completed measures are incorporated into Part A of the DPIA and the corresponding risks from Part C and D are removed. The planned or ongoing measures are included as scheduled mitigations in Part C and D. As a general clarification, Adobe noted that Adobe's commitments should not be interpreted as an acknowledgement of any legal obligation or agreement with the assigned risk levels, and that the improvements *"should instead be viewed in the spirit of making improvements requested by a specific customer with unique requirements due to the context of how they use Adobe services"*.[448]

[446] Overview of Data Protection Harms and the ICO's Taxonomy Information Commissioner's Office Date: April 2022, URL: https://ico.org.uk/media2/migrated/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf.

[447] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025.

[448] September 2025 Response to SURF Concerning Technical Mitigations (4 Oct 2025).

16.2 Identification of the data protection risks

16.2.1 Loss of control – Contractual framework

The contractual framework reflects the terms as negotiated between SURF and Adobe (See also Section 16.1). This risk is specific to SURF's contracts. The contractual provisions discussed below were agreed upon during negotiations between SURF and Adobe in 2022, with certain terms reflecting SURF's preferences at that time.

This framework governing data processing lacks clarity and coherence. Several documents fail to reference or align with one another, and no clear hierarchy is established between them. Some clauses appear potentially contradictory. For example, in addition to Adobe's DPA, for K12 and HED products the Student Data Terms are also applicable. Some clauses in the Student Data Terms differ from those in the DPA, and the terminology used is also inconsistent. The Student Data Terms refer to 'Student Data' and 'Student Assets', while the DPA focuses on 'Customer Data' even though they ultimately refer to the same, or at least overlapping, categories of personal data. The Student Data Terms also link to Adobe's General Terms of Use (ToU), not the General Terms that are part of the Enterprise Licensing Terms.

If there is any conflict between the terms in the General Terms and the Product Specific Terms (in this case the Student Data Terms), then the Product Specific Terms govern in relation to those Services or Software.[449] The Student Data Terms also take precedence over Adobe's Privacy Policy.[450] There is no clause establishing the hierarchy between the Student Data terms and Adobe's DPA. Adobe's Enterprise Licensing Terms, its General Terms, and Specific Product Licensing Terms are not mentioned in the Student Data Terms.

An example of the uncertainty this creates is that the General Terms suggest Adobe will use anonymised personal data for publishing and distribution (in a broadly formulated purpose), but the Student Data Terms (Article 6.1) reveal that this data can be re-identified, indicating it remains pseudonymous personal data under the GDPR. In addition, Adobe reserves the right to re-identify this data when "permitted or required by law" without specifying the circumstances and claims to have no obligation to delete the de-identified data.

This ambiguity creates legal uncertainty regarding the allocation of roles (see also Risk 2), responsibilities, and applicable data protection obligations. Under Article 28 of the GDPR and the accountability principle, a controller must be able to demonstrate that processing by its processor is carried out under clear, documented instructions. The agreements do not provide the level of clarity, consistency, or coherence required to ensure that the controller's instructions are properly documented. As a result, the educational institution cannot be certain that Adobe processes personal data in line with their intended instructions, and Adobe may rely on conflicting terms when carrying out its duties.

The probability of the risk occurring is more likely than not as the contractual framework is not coherent. The impact for the rights and freedoms of data subjects could be significant, as it can

[449] Article 1.2 'Product Specific Terms, Adobe General Terms of Use, Effective as of 18 June 2024, URL: https://www.adobe.com/legal/terms.html.

[450] Preamble of the K-12 (Primary and Secondary) and Higher Education Product Specific Terms for Student Data, Last updated June 18, 2024, URL: https://wwwimages2.adobe.com/content/dam/cc/en/legal/servicetou/Adobe-EDU-Terms-en_US-20240618.pdf.

manifest a variety of issues, including inconsistent safeguards, processing beyond what was authorised, unclear accountability, and obstacles in exercising their rights. Considering both the probability and the potential for significant impact, this results in a high risk.

While Adobe disagrees with the risk assessment, Adobe indicated a willingness to work with SURF on the contractual framework and to consider the suggested measures.

16.2.2 Loss of control – Role division

The contractual framework reflects the terms as negotiated between SURF and Adobe (See also Section 16.1). This risk is specific to SURF's contracts. The contractual provisions discussed below were agreed upon during negotiations between SURF and Adobe in 2022, with certain terms reflecting SURF's preferences at that time.

According to Article 28 (3) GDPR, data processing agreements should define the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the rights and obligations of the controller.

It was agreed during negotiations between SURF and Adobe that Adobe's standard DPA would apply. However, this standard DPA lacks in several aspects. The DPA does not serve as a proper instruction from the educational institution as controller to Adobe as processor, as it fails to define the personal data involved (it includes examples of data that is typically processed in Adobe's products) and describes the purpose of the processing in overly broad terms. This lack of specificity leaves room for interpretation.

The current wording in the DPA is so broad that it allows Adobe to perform almost any activity in various roles. The lack of specificity not only makes it difficult to factually establish whether the DPA correctly reflects the roles of controller and processor but also influences the ability to assess the legal basis for processing (and who must have the legal basis for the processing). When Adobe acts as an independent data controller, the education institution must have a valid legal basis for disclosing personal data to Adobe as a third party. Secondly, Adobe must have a legal ground for all the data processing, including 'further' processing for its own purposes. 'Further' processing is only allowed if it is compatible with the initial purposes of the data collection.

While Adobe's standard DPA creates uncertainty about who the controller and processor are for specific processing activities, other factors also contribute to the ambiguity. SURF's agreement with Adobe (see Section 1.5.2) states that Adobe is the Consortium Member's data processor, and the Consortium Member is the data controller in connection with the collection of Student personal data *"in the Offering and in another Adobe application that Consortium Member allows K-12 Students to access".* For further details about how Adobe collects, uses, and discloses personal data collected from Students it refers to Adobe's Privacy Policy, which lists Adobe's data processing operations as data controller. Adobe clarified that *"they only point to the Adobe Privacy Policy for "further details"- when it comes to processing as a processor, the Data Processing Agreement together with the General Terms is instructive."* [451] While this may be the case, Adobe's general privacy policy covers a wide range of data processing activities, many of which go beyond those strictly related to the provision of the services. As a result, referring to this privacy policy does not clarify the processor specific processing activities. Instead, it

[451] Email Adobe 28 March 2025.

introduces confusion and blurs the distinction between the roles and responsibilities of the parties.

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 based on factual circumstances.

Adobe offers its products to both consumers and enterprises, using a (largely) shared infrastructure and code base. Although Adobe does try to make a split between consumers and enterprises, for instance by disabling certain data collection for enterprises and by giving enterprises more control over user assets in their 'enterprise storage model', the shared model can cause issues in practice when not all data collection features are disabled or Adobe uses enterprise data for their own purposes in other ways. Such situations can easily arise given the overlap with consumer products, where Adobe will always act as a controller.

This DPIA revealed that some personal data is processed by Adobe as a controller, while Adobe should process this data in the capacity of processor on behalf of the educational institution (this includes identifiers and contact information, content used to deliver features requested by the user, profile data, service account details and Adobe identity data).

It is certain that the roles of the parties are not clear and that some data should be processed by Adobe as a processor instead of a controller. It is also certain that the current contractual framework is inadequate. This can have a severe impact on several rights and freedoms of the data subjects. The risk can be qualified as high.

While Adobe does not agree with the risk assessment, Adobe indicated that they are open to providing further clarification on the categories of personal data processed for their own purposes as part of any future contractual discussion.

16.2.3 Loss of control – Adobe's use of Customer Data to enforce its rights under the Agreement

Adobe is permitted to use Customer Data to enforce its rights under the Agreement. It is unclear what exact data is involved, how it will be processed, or under what circumstances. Enforcing rights could encompass a wide range of actions, from litigation and debt collection.

Adobe relies on its legitimate interests for this purpose. It is Adobe's legitimate interest to protect its interests. "Enforce its rights" can be interpreted widely and potentially can influence data subject's rights. The broad phrasing of this purpose leaves too much room for interpretation and does not sufficiently safeguard the rights and freedoms of the data subjects.

In response to the full draft of this DPIA, Adobe argued that *"Adobe has a legitimate interest in protecting its commercial interests including pursuing contractual breaches and ensuring that customers comply with the terms of the agreement that they have signed. Indeed, the freedom to conduct a business and the right to an effective remedy are Charter protected rights. The GDPR explicitly notes that it respects and observes such rights (recital 4). Moreover, the enforcement of civil law claims is also recognised in the GDPR as a legitimate potential restriction on data subject rights and controller obligations."*[452]

[452] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025

However, this does not change that the phrasing "to enforce its rights under the agreement" is too broad. It is drafted in a way that could allow almost any form of data processing to be justified under an open-ended notion of "enforcement", without adequate limitation or transparency. Adobe also referred to Adobe's Privacy Policy which includes the following wording: *"In connection with legal claims, compliance, regulatory and investigative purposes as necessary (including disclosure of information in connection with government agency requests, legal process or litigation)."* This clause is also formulated in broad "catch-all" terms and similarly fails to impose any meaningful limits on the scope of the processing.

While Adobe's underlying legal basis may be valid in principle, the clause as written remains overly vague. The explanations by Adobe do not meaningfully narrow the scope of the clause or provide the level of specificity required to ensure that the processing is proportionate and meets the principal of purpose limitation.

There is a reasonable occurrence of the risk that Adobe uses Customer Data to enforce its rights under the agreement which potentially can (negatively) influence data subject's rights and freedoms since Adobe is contractually allowed to do so in the current contractual framework. Therefore, this constitutes a high risk.

Adobe disagrees that this contractual term presents a high risk to the rights and freedoms of individuals but is nonetheless willing to discuss with SURF any specific contractual language on this point as part of the ongoing contract renewal negotiations.[453]

16.2.4 Lack of transparency – List of sub processors is incomplete

The list of third-party sub processors is not complete. The list mentions Akamai, Cloudflare and Fastly, but it does not specify that they are used for the services assessed in this DPIA, while traffic to these service providers was observed. In other words: these service providers are identified in Adobe's sub processor list (with a description of the processing they do, their full company name and the countries in which they provide services from) but not correctly associated as sub processors for specific Adobe Services.

The probability that this risk occurs is more likely than not, since it is the factual situation. Given the type of services (CDN providers) and the fact that these subprocessors are listed, the main concerns relate to transparency (Articles 12-14 GDPR) and accountability (Article 28 GDPR). The information is not entirely absent and existing agreements between Adobe and the sub-processors mitigate the potential effect on data subjects' rights. The risk can therefore be qualified as low.

In response to the full draft of this DPIA, Adobe has committed to update the sub-processor list by the end of 2025. Adobe has updated the subprocessor list as of December 2025 to address the flagged issues.[454] It does seem that the 'Description' column was not (fully) updated. E.g., for Cloudflare it states "Adobe does not route user information through Cloudflare" but in reality, Adobe's main authentication page (auth.services.adobe.com) is routed through Cloudflare and thus processes user credentials. For Fastly the description only mentions Adobe Experience

[453] Feedback Adobe 18 December 2025.

[454] September 2025 Response to SURF Concerning Technical Mitigations (4 Oct 2025), and Feedback 18 December 2025.

Cloud. So, while there are improvements made in this area, the descriptions still need to be completed to lower the probability of the risk occurring.

16.2.5 Loss of control - Not aware and thus not able to object to proposed changes subprocessors

Pursuant to Article 28(2) of the GDPR, a data processor shall not engage another processor without the prior specific or general written authorisation of the controller. In the case of a general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of the other processors, thereby giving the controller the opportunity to object to such changes. The educational institution provides a general written authorisation through Adobe's DPA. Adobe commits to enter into a written agreement with each subprocessor imposing equivalent or stronger data protection and security measures.

Adobe maintains lists of subprocessors involved in the processing operations. This list is available through a public facing website. To receive notice of the proposed changes to the list, Adobe provides the Customer with at least fourteen days' notice if the Customer has subscribed for updates. If an educational institution does not opt in for the notifications, they will not be aware of the proposed changes and are unable to assess whether a new subprocessor can process personal data in accordance with the terms of the DPA. As a result, they may miss the notice period and lose the opportunity to object to the engagement of the new subprocessor in time.

In response to the full draft of this DPIA Adobe argued that Adobe's mechanism for notifying controllers about changes of subprocessors is compliant with Article 28 (2) GDPR and EDPB's Guidelines 07/2020 and Opinion 22/2024. While it may be compliant, if educational institutions are not aware that they need to sign up for notifications to get information about new subprocessors, they are not able to object to the proposed subprocessors within the (already short) 14-day period. For that reason, this risk is flagged in this DPIA (for awareness).

The probability of this risk occurring is reasonable, as the notifications require an active opt-in. The impact for the rights and freedoms of data subjects if the risk occurs is low, because Adobe has listed strict and adequate requirements for subprocessors that must be met. These include requirements on privacy and data protection. This risk can therefore be qualified as low.

Adobe noted SURF's mandated contracting structure and Adobe's earlier, rejected proposal for a unified DPA in relation to this risk. SURF's current approach could allow some members to block a new subprocessor while others accept it, which is impractical for Adobe. All educational institutions are independent controllers, and this practical issue does not change that each controller should have the opportunity to object to subprocessors.

16.2.6 Loss of control – Adobe's cookies

During testing, Privacy Company observed multiple instances where the cookie banner was not working as expected. In case of Adobe Stock, several advertisement networks were included even when the user did not consent to marketing cookies (see Section 2.3.1.6). During a visit to Adobe Express, Google DoubleClick cookies (an advertisement network) were observed (see Section 2.3.2.7). Several cookies were misclassified or not classified in the cookie banner (e.g., see Section 3.2.1.1) and the cookie banner uses vague and generic terms for the purposes (see Section 11.3.1). Furthermore, the Adobe Cookie Policy fails to provide a comprehensive list of cookies, technologies, and their retention periods and uses similar generic purpose descriptions, lacking transparency (see Section 14.2.1).

Adobe promptly addressed the non-functional cookie banner instances and the misclassified cookies. Also, they implemented a technical feature that makes it impossible for educational users to opt-in to personalised advertising cookies. This reduces the risk that users are profiled without valid consent.

Despite the substantial improvements that Adobe has made, the purposes described for cookie use remain vague and generic. As a result, there is a reasonable probability that students and children (who are less equipped to understand unclear privacy information) may experience a loss of control due to insufficient transparency. However, the impact on educational users' rights and freedoms is now low. Because they can no longer opt-in to personalized advertising cookies, the practical consequences of inadequate information are limited, and users cannot unintentionally consent to high-risk processing. The risk can be qualified as low.

In response to the full draft of this DPIA, Adobe informed SURF that it will be implementing (Q1 2026) enhancements to the current scanning and review process under which sites and webservices will be scanned, and issues resolved, quarterly on a rolling basis.[455]

16.2.7 Loss of control – Reporting to NCMEC

Adobe reports all CSAM confirmed by its Trust and Safety team to NCMEC as required by US federal law, with no exceptions. Adobe confirmed that its Trust and Safety team is trained to recognize CSAM according to the US legal definitions, which applies a general standard. An image removed for violating Adobe's terms would not be reported to NCMEC unless it was CSAM.

Adobe relies on its legitimate interests for these reports to NCMEC but does not perform individual balancing tests. Sharing information with NCMEC can have severe consequences for data subjects, particularly in cases of false positives, as it may trigger criminal investigations and lasting reputational harm. While Adobe's thorough human review process significantly reduces the probability of erroneous reports, the potential impact of such erroneous reports on data subjects remains high. The combination of remote likelihood and potentially serious impact constitutes a low risk according to the risk matrix (see Section 0).

16.2.8 Disclosure of user data to foreign law enforcement by Adobe as controller

Adobe relies on the legal basis of Article 6(1)(c) GDPR to respond to requests from government or law enforcement agencies during investigations and to use or share data as necessary to detect, prevent, or address fraud, security threats, illegal or deceptive activities, misuse of its services and software, or technical problems such as software piracy.[456]

Adobe commits to redirecting Government and Law Enforcement Inquiries ("Third-Party Demand") to the Customer. If that is not possible, Adobe will, to the extent legally permitted to do so, provide the Customer reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Customer to seek a protective order or other

---

455

456 Adobe Privacy Policy, 'How does Adobe use the information it collects about you, and what are the legal bases for these uses?', Last updated: June 18, 2024, URL: https://www.adobe.com/privacy/policy.html#how-does-adobe-use-the-information-it-collects-about-you-and-what-are-the-legal-bases-for-these-uses.

appropriate remedy.[457] These guarantees only apply to the Customer Data, not the other categories of personal data that are processed by Adobe for the provision of the services.

According to the Government Requests Transparency Report is from Adobe's Fiscal Year 2023 most of the legal processes Adobe has received are related to online child safety. 42% (65 out of the 156 total requests Adobe received) of legal requests were follow-ups to CyberTips Adobe has sent to the NCMEC (see also Sections 7.3.1 and 9.3.2).

If a law enforcement request originates from a third country (for example the requests that are made as a follow up to the tips Adobe sent to the NCMEC), the disclosure of personal data cannot automatically be based on Article 6(1)(c) GDPR, as such legal ground only applies when the obligation stems from EU or Member State law (including the implementation of an international agreement, which makes such request binding and enforceable under EU or Member State law). In situations where disclosure based on an international agreement is not mandatory, but such cooperation is permitted under EU or Member State law Article 6(1)(e) GDPR (public interest) could apply.[458]

If both Article 6(1)(c) and (e) GDPR are not available for Adobe, Adobe may still have a legitimate interest in responding to a request from a third-country authority, especially when subject to foreign laws where non-compliance could result in sanctions. However, to rely on Article 6(1)(f) GDPR any such processing must be necessary and carefully weighed against the data subject's fundamental rights and freedoms. The EDPB, in a specific situation, has previously taken the view that the interests or fundamental rights and freedoms of the data subject, under those particular circumstances, would override the controller's interest in complying with a request from a third country law enforcement authority to avoid sanctions for non-compliance.[459]

In response to the full draft of this DPIA, Adobe confirmed that *"no notifications have ever been made to any SURF educational institutions under this clause [Article 9.5 Adobe DPA] nor do any of our transparency reports dating back to 2014 identify any law enforcement requests from the Netherlands nor do they identify any relating to individuals in the Netherlands."*[460]

Without a valid legal ground under the GDPR disclosing data in response to these requests would be unlawful, and in other ways also significantly impacting the rights and freedoms of the data subjects. However, as Adobe had not had any law enforcement requests relating to individuals from the Netherlands (since 2014), the probability of the risk occurring is low. The combination of remote likelihood and potentially serious impact constitutes a low risk according to the risk matrix (see Section 0).

16.2.9 Loss of control – File sharing by users

Adobe Creative Cloud has several issues related to file sharing and project visibility. Original project creators are not notified when access is granted to others by an administrator. Users can also not easily see which files they have shared, especially when files are shared broadly (with

[457] Article 9.5 Adobe DPA.

[458] EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, nr. 133 and 134, URL: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf.

[459] Idem. Nr. 136, and see the annex to the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection

[460] Adobe response to SURF additional questions 8 August 2025 (17 Oct 2025).

the whole organisation or anyone). Testing showed that in some cases documents cannot be unshared due to a broken functionality, leaving deletion as the only workaround to stop sharing the document with other users.

Given the confirmed limitations in the software and the known issue with the unshare button, it is likely that these issues will occur when using the product. these shortcomings undermine the user's control over data access. The impact on the rights and freedoms will be limited as the user can still undo the sharing by deleting the document. The data protection risk is low.

Adobe has confirmed they are working on improvements in this area,[461] but the risk is included in the DPIA to ensure it is monitored and addressed. Adobe further stated:

> *"Work is planned to improve the UX in Adobe Home (web and desktop) in order to indicate that a file (a) has not been shared/is only visible to the creator; (b) has been shared and is either public, accessible by anyone within an entire organization, or only accessible by specific users – and whom."* [462]

And:

> *"Adobe will implement changes to fix an incorrect configuration related to sharing options for Adobe Express and Adobe Photoshop files in Creative Cloud. This fix will address your finding, allowing users to directly change file sharing settings for Adobe Express and Adobe Photoshop files from the Creative Cloud desktop app and Adobe Home on the web."* [463]

This work will be completed before end of 2026 and includes enhancements on reminding users which documents were shared publicly.

16.2.10 Loss of control – Accessibility projects and files by administrators

Administrators can view project names and projects and access certain Creative Cloud files by using URL identifies and log data (see Section 3.2.3.2 and Section 3.1.11) without the user's knowledge. This is not clearly communicated to the user and can lead to a false sense of privacy and control. Although partially documented (in the collaboration FAQ), it does not align with user expectations, or the assurances made in the security white paper.

Adobe notes that transparency obligations under Articles 13 and 14 GDPR lie with the controller and that Adobe supports compliance through product documentation, without assuming responsibility for how controllers fulfil these duties.[464]

For the purposes of this DPIA, however, the assessment focuses on risks to data subjects arising from the use of Adobe Creative Cloud (and Document Cloud). This includes identifying any practical difficulties controllers may encounter in meeting their transparency obligations due to the product's design or operation, as such difficulties can still result in risks for data subjects.

---

[461] Email Adobe to SURF, 28 March 2025: *"We are aware of this, and investigations are underway to incorporate the capability to show when the document is shared in all cases in the referred list view. "*

[462] September 2025 Response to SURF Concerning Technical Mitigations (4 Oct 2025).

[463] Response to SURF Concerning Technical Mitigations (31 October 2025).

[464] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025.

The probability of the occurrence of the risk that administrators access files of users without the user's knowledge is reasonable as it is technically possible, and the users are not made actively aware of the fact that someone accessed their files. The impact of the occurrence of the risk is high.

In response to the full draft of this DPIA, Adobe confirmed that the Adobe Creative Cloud security overview is being updated to accurately describe the current state and is expected to be finalised by the end of 2025.[465] While the information is helpful, the educational institutions need to take some steps (measures) to lower the probability of the risk occurring and to reduce the risk.

16.2.11 Loss of control – User is not aware that functionalities are offered by an online service

Several features in Acrobat and Photoshop connect to the Adobe Cloud to perform actions. Sometimes the user has an option to disable the online functionality or choose between a local or online implementation. In other cases, the user is not directly aware that the functionality is offered by an online service (or a so called 'on-demand service'). An example of the latter is the Firefly AI functionality discussed in Section 8.1, which cannot be disabled by the end-user. Users are not made aware of what functionality in the desktop apps is offline, and what functionality is online/cloud-backed (and thus sharing data with Adobe). There is no publicly available information that distinguishes the features that are included in the on-premise applications from those that are available as additional on-demand options.

Given that users are not clearly informed about which functionalities are offline versus hosted on the cloud storage side, there is a reasonable probability of the risk that users may unintentionally share data with Adobe through cloud services, unaware of the online functionality. The lack of transparency can lead to unintentional data sharing, and as a result Adobe's DPA becomes applicable to the processing of the data. This means that Adobe may use the data for its own purposes as outlined in the general terms. The impact on the rights and freedoms of data subjects is high, because a lack of transparency is a violation of a principle of the GDPR. The risk can be qualified as high.

In response to the full draft of this DPIA Adobe notes that the transparency obligations lie with the controller and that this risk/finding seems to be aimed more toward the educational institution rather than Adobe.[466] While it is true that the controller is responsible for ensuring transparency, if the information is unclear or not visible in the interface the educational institution cannot meet its transparency obligations. Despite Adobe's view, Adobe committed to enhance existing documentation to provide additional detail about Creative Cloud applications in the first half of 2026.[467]

16.2.12 Loss of control – Users restricted in the ability to delete documents

Users can be restricted in their ability to delete documents. For example, creating a project library with *restricted* permissions leads to problems when the creating user chooses to *'Leave'* the library (which is the only option the Creative Cloud web application offers for such libraries,

[465] Response to SURF Concerning Technical Mitigations (31 October 2025).

[466] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025.

[467] September 2025 Response to SURF Concerning Technical Mitigations (4 Oct 2025).

as the *'Delete'* option is only available in the desktop interface, see Figure 36). In these cases, their own permissions are removed, and they are no longer able to remove the library or files in that library. This can lead to a situation where none of the users in the organisation is able to remove the files from the library and the only option is to delete the whole project containing the library. This lack of control may result in documents longer being stored than necessary.

Adobe argues that the GDPR does not require controllers or processors to provide self-service deletion tools in user interfaces. It cites EDPB guidelines stating controllers have flexibility in how they accommodate data subject rights, including through manual processes, and notes that Adobe does provide a deletion facility.[468]

The risk however is not about lacking self-service tools. It is that the permission system can lock out all users from deleting certain files. When this happens, entire projects must be deleted to remove the files inside.

The probability of the occurrence of the risk is reasonable due to the current technical limitations. The impact on the rights and freedoms will be limited as the user can still delete the document by deleting the project. This workaround may be impractical, especially if it means that many other documents are deleted together with the project. The data protection risk is low.

Despite its disagreement with the risk, Adobe committed to update Adobe Home to match the experience of deleting libraries that were created inside a project from Adobe Creative Cloud Desktop in 2026.[469]

16.2.13 Disproportionate processing of telemetry data

As described in Section 2.3.1.1, Adobe defines some forms of collected telemetry as essential and does not allow these types to be disabled. As described in Section 14.2.2, Adobe is shown through the DSAR responses to collect additional data types that conflict with Adobe's statement that that 'desktop app usage data' is not collected for business profiles'.

Adobe does not provide a comprehensive description of what telemetry is mandatory. Adobe additionally states that with business profiles, only essential telemetry is collected, and that personal accounts can opt-out of telemetry. Privacy Company conducted tests with enterprise licenses and business profiles and observed a considerable amount of telemetry. It is not clear from Adobe's responses to SURF or Adobe's documentation if this telemetry is all considered 'essential', or if it was collected by mistake.

Additionally, Adobe states that it stores telemetry for four years. Adobe does not provide specific reasoning for this storage period or explains why the same storage period is used for all data types included in telemetry. Because much of the data processed on behalf of educational institutions is data from students, and students may graduate and thus lose their Adobe accounts within a four year period, the storage is disproportionate. The telemetry will likely be stored after a user account has been deleted. Without a specific description of the purposes for which the telemetry is processed, it is not possible to assess the proportionality.

[468] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025.

[469] Response to SURF Concerning Technical Mitigations (31 October 2025).

Privacy Company's test simulated the minimum amount of telemetry and other data shared from business profiles to Adobe. Because the observed telemetry cannot be disabled by a business profile, the likelihood of this data being collected is high. Adobe does not provide explanations of which telemetry is essential, or why, or of its intended use. The storage period of the telemetry is long enough that it will likely be stored longer than many of the students' accounts will exist. As described in Table 18, the four year storage period is also true for customer data where Adobe is the controller and customer support data. Like telemetry, this seems disproportionate, and Adobe has not provided an explanation why the data is stored for a period as long as four years.

The processing of the telemetry data constitutes a violation of the principle of data minimization. Moreover, even when the processing of telemetry data would be necessary, the retention period constitutes a violation of the principle of storage limitation. Because the violation of these principles is highly likely during typical use of Adobe services by educational institutions, the risks to data subjects is high.

In response to the full draft of this DPIA Adobe explained that *"student users with only an Adobe ID provisioned to them by an educational institution have usage data collection for product improvement turned off automatically. SURF, however, identified a situation in which a user with both an individual consumer ID and a student user ID would have the choices as to collection of usage data for product improvement in the school provisioned version of the product determined by the consent choice made in the individual consumer ID account.*

Work is planned to address this situation and when completed, Adobe will exclude ALL student profiles from desktop usage data collection for product improvement, whether or not a student also has an individual consumer user Adobe account. This is the only use case today where desktop usage data may be collected for a student. After this change, students will be opted out of desktop usage data collection for product improvement in all cases."[470]

16.2.14 Disproportionate processing – Content Credentials

When creating an image with Firefly, Firefly automatically adds Content Credentials to the image. Content Credentials are both attached to the exported image and are stored in the Content Credentials cloud repository (for fully generated AI images), so Adobe can restore Content Credentials when they are stripped from the metadata of the image.

The product's interface does not make it clear to users that content credentials are applied, why they are applied, or how long they will be retained.

Adobe explained that Content Credentials include technical data as well as global user IDs (GUID) and that users may, at their option, provide further information (e.g. names, social media accounts).

In response to the full draft of this DPIA, Adobe explained: *"Adobe's Content Credentials are part of its Content Authenticity Initiative (CAI) — a framework designed to increase transparency and trust in digital content by attaching provenance metadata (e.g., who created, edited, or generated an image, when, and how) which currently has over 4,000 participants from civil society, media, and the technology industry. This is something that is being done entirely to help*

[470] Response to SURF Concerning Technical Mitigations (31 October 2025).

combat misinformation and AI deepfakes. It helps consumers understand if content is AI-generated, edited or original for the social purposes of helping enhance trust. Content credentials are just part of how Adobe offers its services in a responsible manner - to make sure that users cannot easily use Adobe products to create misinformation or other misleading, objectionable or false content (and we would assume these goals are something SURF would generally support, particularly when it comes to allowing students access to this technology).”[471]

Unlike other data items in the Content Credentials, the GUID are only accessible to Adobe, not to the public. Adobe did not explain why it also stores the GUID. Adobe considers the personal data within Content Credentials limited in scope, harmless in nature, and not entirely public. For that reason, Adobe argues that it is very unlikely that the processing of such data will adversely affect users. While it is not clear if the indefinite retention period of the Content Credentials extends to the GUIDs (which are exclusively accessible by Adobe), the indefinite retention of the Content Credentials (including thumbnails) appears disproportionate, especially considering that even intellectual property laws typically impose defined retention periods.

While Adobe relies on legitimate interests as its legal basis, the balancing test would likely not succeed given the lack of storage limitation and the insufficient transparency provided to users.

It is a factual situation that content credentials (including the GUIDs) are stored indefinitely, and that the current interface lacks transparency. Depending on the purpose, this could result in a lack of storage limitation. The impact on the rights and freedoms of data subjects is high, because the lack of storage limitation is a violation of a principle of the GDPR. The risk can be qualified as high.

Adobe has confirmed they are working on improvements in this area and aims to have more information available in January 2026.[472]

16.2.15 Inability to exercise data subject rights – Incomplete DSAR responses Adobe

Data subjects have a right to access personal data concerning them (Article 15 GDPR). As described in Section 2.4, Adobe has responded to two data subject access requests from Privacy Company. In response to these access requests, Adobe has provided various documents with profile information, service information and application log files. Application log files were not provided for all applications, but it is not known if Adobe had other logs available. Adobe also did not provide any personal data processed by third parties as Adobe’s processor, although several of such parties exist (e.g., see Adobe’s explanations in Section 5.3.1.2). The response also included codes that are internal to Adobe for audience segmentation, without an explanation to the data subject as to their meaning (see Section 2.4.3.5). Returning internal codes without explanation does not help the data subject to understand how their data is being used. Individual Generative AI prompts would be part of the Product and Services Data that Adobe processes as controller. The prompts of the test accounts were not returned.

Adobe met the required deadlines and the DSAR response was largely complete, but some relevant data (e.g. generative AI prompts and data shared with third parties) was missing. This indicates a reasonable probability that future DSAR-responses may also omit key information.

[471] Adobe Legal Response to SURF “DPIA Adobe Creative Cloud & Document Cloud” 9 July 2025.

[472] Adobe’s Comments to SURF DPIA v0.5, 18 December 2025.

Missing data, especially if it includes personal insights like generative AI prompts and data shared with third parties, limits the data subject's ability to exercise their rights.

However, Adobe has demonstrated willingness and cooperation throughout the DSAR process. If certain information were not included in the initial response, data subjects would most likely be able to obtain it upon further request. Therefore, while omission may occur, the probability that data subjects ultimately cannot exercise their rights is low. For that reason, the risk is low.

16.2.16 Inability to exercise data subject rights – Administrators not able to honour DSARS
As discussed in 3.1.5.2, In some cases, administrators (as controllers) may need to access files of end-users (for instance, when a user or legal guardian performs a DSAR). Privacy Company has not identified features provided by Adobe to accommodate such scenarios. Adobe suggested that administrators can access documents of end-users directly (which is not the case for Document Cloud documents, and cumbersome for Creative Cloud documents as knowledge of the document identifiers are required). Another suggestion was to use the remove the user account and use the asset reclamation feature, or to force a change of the user's password. Both options seem rather drastic ways to adhere to a data subject access request.

In response to the full draft of this DPIA Adobe referred to Article 28(3)(e) GDPR which states that processors must assist controllers in fulfilling data subject rights through appropriate technical and organisational measures and that the EDPB Guidelines 07/2020 confirm there is no prescribed standard for how convenient this assistance must be. Adobe provides multiple mechanisms for data subjects to access their own data and for admins to respond to requests, which fulfils Adobe's processor obligations (even if some features could be improved for convenience). Adobe argues that because of the existence of these functional methods the risk cannot be characterized as "high", and notes that expanding general administrator access to individual user content could actually increase privacy risks. While certain features might be explored as enhancement request, the current setup is according to Adobe compliant with Adobe's GDPR obligations as processor.[473]

There is no dedicated tool or information available for the administrators to efficiently respond to a DSAR from a user especially when it comes to the retrieval of files, requiring reliance on manual processes and multiple separate mechanisms. While Adobe provides functional methods to access data, manual processes increase the chance of accidental omission or inconsistent data retrieval. There is a reasonable possibility of the occurrence of the risk that the administrator is not able to fully honour a DSAR. This can have a severe impact on the data subjects. The risk can be qualified as high.

Clear information about the limitations of the system, along with dedicated support from Adobe to assist administrators in navigating and completing DSAR requests, would significantly lower the probability of the risk occurring.

16.2.17 Inability to exercise data subject rights – Right to erasure / storage limitation
Adobe has implemented a deletion process for fully removing a user and the user's assets. However, there are scenarios where administrators do not have the option to delete user folders, even after users have been removed from the user list, possibly due to bugs in the software. Moreover, there are scenarios in which the user data removal does not work. The tests

[473] Adobe Legal Response to SURF "DPIA Adobe Creative Cloud & Document Cloud" 9 July 2025.

showed that users stayed in the 'Active users' list after the user was removed. Administrators must be aware that user folders need to be manually removed after the user account has been removed (in those cases it takes another 14 days for the data is deleted). If this is not done, user data will be kept indefinitely, and this is not always clear from the documentation. A similar issue arises when Enterprise or Federate ID type users have multiple organisation memberships. For these cases, fully removing an Enterprise or Federated ID requires the administrators to delete the user from three places: the user list, the Business ID directory, and the domain directory. Finally, Adobe's documentation contains conflicting information about the process of permanently deleting or reclaiming data and digital assets.

Given the technical constraints and the unclear and inconsistent instructions on how to delete the data, it is likely that data might not be (completely) deleted. Incomplete or ineffective deletion can affect the data subject's right to erasure as well as the principle of storage limitation. This qualifies as a high risk to data subjects.

In response to the full draft of this DPIA Adobe has informed SURF that it is developing a capability that will enable admins to more easily remove assets for users that have been removed from the organization by allowing the admin to configure a retention policy for asset deletion after a user has a status of "inactive" (i.e., removed from the org). This is scheduled for 2026.[474] As part of these improvements, Adobe has already released Adobe Admin APIs for Storage Management[475], enabling customers to use an API to configure a retention policy for inactive users' assets that are stored in enterprise storage through an API call.[476] When the work is completed, it is still up to the educational institutions to implement the measures suggested in Section 17.

[474] Response to SURF Concerning Technical Mitigations (31 October 2025).

[475] 'Adobe Admin APIs for Storage Management', URL: https://developer.adobe.com/adobe-admin-apis-storage-management, last viewed: 26 November 2025.

[476] Response to SURF Concerning Technical Mitigations (31 October 2025).

16.3 Summary of risks

By representing the risks encountered according to their potential impact on the rights and freedoms of data subjects, a picture of the high and low risks associated with processing personal data in Creative Cloud emerges. This is displayed in the risk graph developed by the UK regulator ICO, as follows:

Table 19: Risk matrix based on the ICO model

Severity of impact	Serious harm	**Low risk** 7, 8, 15	**High risk** 3, 10, 11, 16	**High risk** 1, 2, 13, 14, 17
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk** 5, 6, 9, 12	**Low risk** 4
		Remote	Reasonable possibility	More likely than not
	Likelihood of harm			

17 Risk mitigating measures

17.1 Measures to be taken to mitigate privacy risks

The table below show the 17 data protection risks for data subjects, with the mitigating measures Adobe and the educational institutions can take. Where an indication of the timeline for measures to be taken by Adobe is available, the estimated timeframe is shown in bold.

Table 20: Overview suggested mitigating measures

No.	Risk	Measures
1.	Loss of control – Contractual framework	**Measures Educational Institutions**
		Agree on contractual purpose limitation. Explicitly define roles and responsibilities. Amend contract and DPA. Establish retention periods.
		Measures Adobe
		Establish a clear hierarchy between terms.

		Identify inconsistencies and harmonize terms. Amend contract and DPA. Establish retention periods. **The suggested measures will be part of the discussion in the context of the current contract renewal.**
2.	Loss of control – Role division	**Measures Educational Institutions**
		Explicitly define roles and responsibilities. Contractually limit the processing of Customer Data by Adobe. Include an exhaustive list of legitimate business purposes that clearly defines limitations on the categories of personal data processed, processing activities permitted, and retention periods for each purpose. Pay special attention to: - Product improvement and development - Statistics / anonymized information - To enforce its rights under this Agreement - General communication to users - Storage of content credentials - Fraud prevention, security, and misuse detection (including detection, review and reporting of illegal content) - Reporting illegal content. - legal compliance and responding to government requests.
		Measures Adobe
		Explicitly define roles and responsibilities. Present the controller with a detailed description of the service to enable the controller to define the purpose and the personal data processed for this purpose. **The suggested measures will be part of the discussion in the context of the current contract renewal.**
3.	Loss of Control - Adobe's use of Customer Data to enforce its rights	**Measures Educational Institutions**
		Restrict Adobe from using Customer Data for this broad purpose.
		Measures Adobe

		Do not use Customer Data for enforcing Adobe's rights. **The suggested measures will be part of the discussion in the context of the current contract renewal.**
4.	Lack of transparency – List of sub processors is incomplete	**Measures Educational Institutions**
		Exercise the audit right to regularly audit which subprocessors are used.
		Measures Adobe
		Provide transparency on the applicable subprocessors and maintain a complete list (**End of 2025**).
5.	Loss of control - Not aware and thus not able to object to proposed changes sub processors	**Measures Educational Institutions**
		Ensure to sign up to receive the notifications.
		Measures Adobe
		Send the updates on subprocessors by default to the vendor compliance / purchase department.
6.	Loss of control – Adobe's cookies	**Measures Educational Institutions**
		Regularly audit the web traffic for not listed cookies.
		Measures Adobe
		Comply with the legal transparency requirements about cookies and similar technologies (improve explanation in Cookie Consent Manager and Cookie Policy). Implementing enhancements to the current scanning and review process **(Q1 2026).**
7.	Loss of control - Reporting to NCMEC	**Measures Educational Institutions**
		For use cases / school assignments involving content that could infringe Adobe's policies (such as certain art projects or creative assignments involving potentially controversial themes or nudity): - exclusively work in desktop applications, and - disable the use of cloud storage or only store files locally.
		Measures Adobe
		Perform an individual legitimate interest balancing test before each report to NCMEC.
8.	Disclosure of user data to foreign law enforcement by Adobe	**Measures Educational Institutions**
		For use cases / school assignments involving content that could infringe Adobe's policies (such as certain art projects or creative assignments involving potentially controversial themes or nudity):

		- exclusively work in desktop applications, and - disable the use of cloud storage or only store files locally.
		Measures Adobe
9.	Loss of control – File sharing by users	**Measures Educational Institutions**
		Encourage periodic review of which documents have been made public and implement manual removal procedures for public documents after a given period of time.
		Measures Adobe
		Provide clear messaging to users about which documents are shared publicly. **(End of 2026)** Provide prompts to users reminding them which documents are shared publicly. **(End of 2026)** Provide users the option to limit the amount of time a document is available publicly at the moment of sharing. Notify project creators when administrators change access rights over works
10.	Loss of control – Accessibility projects and files by administrators	**Measures Educational Institutions**
		Create internal policies wherein administrators notify creators of works when access rights have changed. Create internal policies that inform users who within an organisation can access their files at time of creation.
		Measures Adobe
		Notify project creators when administrators change access rights over works. Notify users when administrators access files and inform users that administrators can access files at the time of file creation.
11.	Loss of control – User is not aware that functionalities are offered by an online service	**Measures Educational Institutions**
		Clearly describe the key functionalities (including on-demand services).
		Measures Adobe
		Provide users with documentation and popups that inform them which functionality in desktop apps is offline, and which is shared with Adobe.
12.		**Measures Educational Institutions**
		Inform users of the current technical limitations.

	Loss of control – Users restricted in the ability to delete documents	**Measures Adobe**
		Allow users to 'Delete' items in the Creative Cloud web application in the same manner as the desktop application **(End of 2026)**.
13.	Disproportionate processing of telemetry data	**Measures Educational Institutions**
		Opt out from optional telemetry when and where the option is made available.
		Measures Adobe
		Reduce the storage period of all telemetry Clarify what telemetry is considered mandatory, and what is considered optional Delete telemetry when user accounts are deleted Do not collect unnecessary telemetry, and define clearly what is necessary and what is not Publish and update a list of telemetry, clarify which is mandatory, and why. Additionally clarify which forms of telemetry are collected when the user has opted in. Do not collect telemetry from desktop application when used by students **(End of 2026)**.
14.	Loss of control – Content Credentials	**Measures Educational Institutions**
		-
		Measures Adobe
		Inform users about what is stored, for how long, for what purposes and who has access to that data (before they generate images). Do not store thumbnails, at least not for non-AI or partially AI content. Establish (not indefinite) retention periods for content credentials (especially for user IDs and thumbnails). Anonymize data after a certain period of time or delete it all together. Bring Content Credentials fully in line with the Code of Practice for AI Act article 50, when it comes into force in 2026.
15.	Inability to exercise data subject rights – incomplete DSAR responses Adobe	**Measures Educational Institutions**
		-
		Measures Adobe

		Provide complete data in the DSAR response. Provide complete descriptions / give sufficient context for the data subject to understand the returned data (for example explanations for internal codes). Continue to provide clear follow-up support to data subjects by answering any clarifying questions regarding their DSAR responses, ensuring they understand the information provided.
16.	Inability to exercise data subject rights – Administrators not able to honour DSARS	**Measures Educational Institutions**
		Create and maintain a dedicated process to handle DSARs from users.
		Measures Adobe
		Provide tooling for administrators to answer DSARs of data subjects. Provide clear guidance on system limitations. Ensure dedicated support from Adobe is available to assist administrators in navigating and completing DSAR requests.
17.	Inability to exercise data subject rights – Right to erasure / storage limitation	**Measures Educational Institutions**
		Create a clear work instruction around user deletion and user asset deletion. Ensure that users are removed from the 'Active users' lists after the user was removed. Use the Adobe Admin APIs for Storage Management to configure a retention policy for inactive users.
		Measures Adobe
		Simplify process of removing users, offering a way to remove a user and all of its directory entries **(End of 2026)**. Update documentation to match the reality of the deletion process **(End of 2026)**. Inform administrators explicitly that assets are kept when a user is deleted. Remove a user's assets along with the user account.

17.2 Assessment of risks after taking mitigating measures

This DPIA has identified 9 high risks and 8 low risks to the rights and freedoms of individual data subjects. For each risk mitigating measures have been identified. The types of measures differ in their nature. If all the measures can be taken, the risks will be mitigated and only low risks remain. After implementing the mitigating measures, the risks are:

Table 21: Residual risks after mitigation

Severity of impact	Serious harm	**Low risk** 1, 2, 3, 7, 8, 10, 11, 13, 14, 15, 16, 17	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk** 4, 5, 6, 9, 12	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
	Likelihood of harm			

Conclusion

This DPIA has identified 9 high risks and 8 low risks in the use of Adobe's Creative Cloud and Document Cloud. The main causes of these risks are:

- SURF's current contractual framework;
- Product features that restrict data subjects from deleting or unsharing documents;
- Limitations for administrators of institutions in being able to honour the rights of data subjects;
- Disproportionate processing of Adobe's content credentials.

Throughout the DPIA process, Adobe demonstrated a highly constructive and collaborative approach, working closely with SURF to address all identified issues. Adobe assessed the feasibility of the requested technical mitigations and identified which measures it will implement, along with expected timelines. The completed measures have been incorporated into Part A of the DPIA and the corresponding risks from Part C and D have been removed. The planned or ongoing measures are included as scheduled mitigations in Part C and D. As a general clarification, Adobe noted that Adobe's commitments should not be interpreted as an acknowledgement of any legal obligation or agreement with the assigned risk levels, and that the improvements *"should instead be viewed in the spirit of making improvements requested by a specific customer with unique requirements due to the context of how they use Adobe services"*.[477] While not agreeing with all risk assessments or classifications, Adobe has expressed willingness to discuss specific contractual language on several points as part of the ongoing contract renewal negotiations.

Part D of this DPIA outlines technical and organisational measures that can be adopted by the educational institutions, Adobe, or both to mitigate all identified high risks. These measures are expected to reduce risks to a low residual level. In that case, no prior consultation with the Data Protection Authority is required. Although reducing low risks is not strictly necessary, it is recommended because the measures are easy to implement and help better protect the rights and freedoms of data subjects.

As a final note, Adobe Creative Cloud is used in schools to help students create digital art, design, video, and multimedia projects. In art schools or art courses where students explore experimental or provocative themes, educators should be aware that content involving non-reportable child sexualization and extreme sexual content (when reported) may conflict with Adobe's content policies, potentially resulting in account restrictions. Schools should therefore be familiar with these policies when using Adobe's products and services.

[477] September 2025 Response to SURF Concerning Technical Mitigations (4 Oct 2025).