Driving innovation together

DPIA Adobe Creative Cloud & Document Cloud

SURF

Let op: dit is een informele vertaling van het originele Engelse document, bij tegenstrijdigheden is de Engelse versie van de DPIA leidend.

Auteurs: Sanne Ouburg, Mike Noordermeer, Jacob Gursky, Winfried Tilanus, Floor Terra

Versie: 1.01
Datum: 12 februari 2026

Samenvatting

Dit rapport is een Data Protection Impact Assessment (hierna: DPIA) over het gebruik van Adobe Creative Cloud en Document Cloud for Education door onderwijsinstellingen (hierna: instellingen). Deze DPIA is een centrale DPIA, uitgevoerd door Privacy Company namens SURF, de ICT-coöperatie van Nederlandse onderwijs- en onderzoeksinstellingen, die instellingen een algemeen kader biedt voor het beoordelen van gegevensbeschermingsrisico's binnen Adobe Creative Cloud en Document Cloud for Education.

Reikwijdte
Deze DPIA richt zich op Adobe Creative Cloud en Document Cloud for Education. Adobe Creative Cloud for Education is een versie die specifiek is afgestemd op de onderwijssector en de behoeften en eisen van onderwijsinstellingen. Adobe heeft hiervoor verschillende privacybeschermende maatregelen geïmplementeerd. Zo wordt voorkomen dat gebruikers in het onderwijs zich kunnen aanmelden voor gepersonaliseerde advertentiecookies waardoor invasieve gegevensverwerking wordt beperkt. Daarnaast herkent het systeem van Adobe automatisch e-mailadressen van leerlingen in het basis- en voortgezet onderwijs en sluit het deze leerlingen uit van marketingcommunicatie. Hierdoor ontvangen zij uitsluitend essentiële, operationele berichten.

De DPIA beoordeelde het contractuele kader en de bepalingen die tijdens de onderhandelingen tussen SURF en Adobe in 2022 zijn overeengekomen, waarbij een aantal voorwaarden de voorkeuren van SURF weerspiegelden. Het is belangrijk te benadrukken dat de geïdentificeerde risico's binnen dit contractuele kader niet per se wijzen op een breder probleem dat Adobe in algemene zin betreft SURF en Adobe zullen de gesignaleerde risico's adresseren in het kader van de huidige onderhandelingen over de contractverlenging.

Methodologie
Privacy Company combineerde een juridische feitenonderzoekstrategie met een technisch onderzoek van de gegevens die via het gebruik van de producten werden verwerkt. Privacy Company voerde haar beoordeling uit aan de hand van openbare informatie, de documentatie over het systeem (zoals verstrekt door Adobe) en door gebruiksscenario's binnen de producten uit te voeren. Privacy Company diende vervolgens een inzageverzoek in bij Adobe om inzicht te krijgen in welke verwerkingen van persoonsgegevens, waaronder logging en telemetrie, plaatsvonden tijdens de uitvoering van deze scenario's. Er werd ook een technische analyse uitgevoerd om te beoordelen of de waargenomen gegevensverwerkingen overeenkwamen met de beschikbare documentatie. Gedurende 2025 werden verschillende rondes van vragen en feedback over het rapport gehouden, waaronder verduidelijking van kwesties en het zoeken naar oplossingen. Adobe, SURF en Privacy Company hebben ook een bijeenkomst gehouden om de Trust and Safety-maatregelen van Adobe te bespreken, waaronder de CSAM-scanningmethoden en -technieken. Op basis van alle beschikbare informatie wordt in deze DPIA beoordeeld of de gegevensverwerkingen risico's opleveren voor de rechten en vrijheden van betrokkenen.

Resultaat en conclusie: 9 hoge risico's, 8 lage risico's
Deze DPIA heeft 9 hoge risico's en 8 lage risico's geïdentificeerd bij het gebruik van Adobe's Creative Cloud en Document Cloud. De belangrijkste oorzaken van deze risico's zijn:

- Het huidige contractuele kader van SURF
- Productkenmerken die betrokkenen beperken in het verwijderen of niet langer delen van documenten
- Beperkingen voor beheerders van instellingen om de rechten van betrokkenen te kunnen honoreren
- Onevenredige verwerking van Adobe's Content Credentials.

Tijdens het hele DPIA-proces heeft Adobe een zeer constructieve en collaboratieve aanpak getoond en nauw samengewerkt met SURF om alle geïdentificeerde problemen aan te pakken. Adobe heeft de haalbaarheid van de gevraagde technische maatregelen beoordeeld en bepaald welke maatregelen ze zal implementeren, samen met de verwachte tijdschema's. De voltooide maatregelen zijn opgenomen in deel A van de DPIA en de overeenkomstige risico's uit deel C en D zijn verwijderd. De geplande of lopende maatregelen zijn opgenomen als geplande risicobeperkende maatregelen in deel C en D. Ter verduidelijking merkte Adobe op dat de toezeggingen van Adobe niet moeten worden geïnterpreteerd als een erkenning van enige wettelijke verplichting of overeenkomst met de toegewezen risiconiveaus, en dat de verbeteringen *"in plaats daarvan moeten worden gezien in de geest van het doorvoeren van verbeteringen die zijn gevraagd door een specifieke klant met unieke vereisten vanwege de context waarin deze Adobe-services gebruikt*".[1] Hoewel Adobe het niet eens is met alle risicobeoordelingen of classificaties, heeft het bedrijf verklaard bereid te zijn om in het kader van de lopende onderhandelingen over contractverlenging specifieke contractuele bepalingen te bespreken.

In deel D van deze DPIA worden technische en organisatorische maatregelen beschreven die door de onderwijsinstellingen, Adobe of beiden kunnen worden genomen om alle geïdentificeerde hoge risico's te beperken. Deze maatregelen zullen naar verwachting de risico's tot een laag restniveau terugbrengen. In dat geval is voorafgaand overleg met de gegevensbeschermingsautoriteit niet nodig. Hoewel het beperken van lage risico's niet strikt noodzakelijk is, wordt het aanbevolen omdat de maatregelen eenvoudig te implementeren zijn en de rechten en vrijheden van betrokkenen beter helpen beschermen.

Tot slot wordt Adobe Creative Cloud binnen instellingen gebruikt om leerlingen te helpen bij het maken van digitale kunst, ontwerpen, video's en multimediaprojecten. Op kunstinstellingen of in kunstlessen waar leerlingen experimentele of provocerende thema's verkennen, moeten docenten zich ervan bewust zijn dat inhoud met niet-meldingsplichtige seksualisering van kinderen en extreme seksuele inhoud (wanneer gemeld) in strijd kan zijn met het inhoudsbeleid van Adobe, wat kan leiden tot accountbeperkingen. Instellingen moeten daarom bekend zijn met dit beleid wanneer ze producten en diensten van Adobe gebruiken.

[1] September 2025 Reactie op SURF betreffende technische risicobeperkende maatregelen (4 oktober 2025).

De onderstaande tabel geeft een overzicht van de risico's die in deze DPIA zijn geïdentificeerd, de voorgestelde maatregelen voor onderwijsinstellingen en de voorgestelde maatregelen voor Adobe. Wanneer er een indicatie is van het tijdschema voor de door Adobe te nemen maatregelen, wordt de geschatte termijn vetgedrukt weergegeven.

Tabel 1: Overzicht van risico's en voorgestelde risicobeperkende maatregelen

Nr.	Risico	Maatregelen
1.	Verlies van controle – Contractueel kader	**Maatregelen onderwijsinstellingen** - Spreek contractueel doelbinding af. - Definieer rollen en verantwoordelijkheden expliciet. - Wijzig het contract en de DPA. - Stel bewaartermijnen vast.
		Maatregelen Adobe - Stel een duidelijke hiërarchie tussen voorwaarden vast. - Identificeer inconsistenties en harmoniseer voorwaarden. - Wijzig het contract en de DPA. - Stel bewaartermijnen vast. **De voorgestelde maatregelen zullen worden besproken in het kader van de huidige contractverlenging.**
2.	Verlies van controle – Rolverdeling	**Maatregelen onderwijsinstellingen** Definieer expliciet rollen en verantwoordelijkheden. Beperk contractueel de verwerking van klantgegevens door Adobe. Neem een uitgebreide lijst op van legitieme zakelijke doeleinden waarin duidelijk de beperkingen worden gedefinieerd voor de categorieën verwerkte persoonsgegevens, toegestane verwerkingsactiviteiten en bewaartermijnen voor elk doel. Besteed speciale aandacht aan: - Productverbetering en -ontwikkeling - Statistieken/geanonimiseerde informatie - Het afdwingen van Adobe's rechten onder deze overeenkomst - Algemene communicatie met gebruikers - Opslag van inloggegevens voor inhoud - Fraudepreventie, beveiliging en detectie van misbruik (inclusief detectie, beoordeling en melding van illegale inhoud) - Melding van illegale inhoud. - Naleving van wet- en regelgeving en reageren op verzoeken van overheidsinstanties.

		Maatregelen Adobe Definieer rollen en verantwoordelijkheden expliciet. Geef de verwerkingsverantwoordelijke een gedetailleerde beschrijving van de dienst, zodat hij het doel en de voor dit doel verwerkte persoonsgegevens kan definiëren. **De voorgestelde maatregelen zullen worden besproken in het kader van de huidige contractverlenging.**
3.	Verlies van controle - Adobe's gebruik van klantgegevens om haar rechten af te dwingen	**Maatregelen onderwijsinstellingen** Beperk Adobe in het gebruik van klantgegevens voor dit brede doel.
		Maatregelen Adobe Gebruik geen klantgegevens om de rechten van Adobe af te dwingen. **De voorgestelde maatregelen zullen worden besproken in het kader van de huidige contractverlenging.**
4.	Gebrek aan transparantie – Lijst van subverwerkers is onvolledig	**Maatregelen onderwijsinstellingen** Maak gebruik van het recht om regelmatig te controleren welke subverwerkers worden gebruikt.
		Maatregelen Adobe Zorg voor transparantie over de toepasselijke subverwerkers en houd een volledige lijst bij **(Einde 2025)**.
5.	Verlies van controle - Niet op de hoogte en dus niet in staat om bezwaar te maken tegen voorgestelde wijzigingen subverwerkers	**Maatregelen onderwijsinstellingen** Zorg ervoor aangemeld te zijn om meldingen te ontvangen.
		Maatregelen Adobe Stuur de updates over subverwerkers standaard naar de afdeling naleving/inkoop van de leverancier.
6.	Verlies van controle – cookies van Adobe	**Maatregelen onderwijsinstellingen** Controleer regelmatig het webverkeer op niet-vermelde cookies.
		Maatregelen Adobe Voldoe aan de wettelijke transparantievereisten met betrekking tot cookies en soortgelijke technologieën (verbeter de uitleg in Cookie Consent Manager en het cookiebeleid). Implementeer verbeteringen in het huidige scan- en beoordelingsproces **(Q1 2026).**
7.	Verlies van controle - Melding aan NCMEC	**Maatregelen onderwijsinstellingen** Voor gebruikssituaties/ schoolopdrachten met inhoud die in strijd kan zijn met het beleid van Adobe (zoals bepaalde kunstprojecten of creatieve opdrachten met mogelijk controversiële thema's of naaktheid):

		- werk uitsluitend in desktopapplicaties en - schakel het gebruik van cloudopslag uit of sla bestanden alleen lokaal op.
		Maatregelen Adobe Voer voor elke melding aan het NCMEC een individuele afweging van gerechtvaardigde belangen uit.
8.	Openbaarmaking van gebruikersgegevens aan buitenlandse wetshandhavingsinstanties door Adobe	**Maatregelen onderwijsinstellingen** Voor gebruikssituaties/schoolopdrachten met inhoud die in strijd kan zijn met het beleid van Adobe (zoals bepaalde kunstprojecten of creatieve opdrachten met mogelijk controversiële thema's of naaktheid): - werk uitsluitend in desktopapplicaties en - schakel het gebruik van cloudopslag uit of sla bestanden alleen lokaal op.
		Maatregelen Adobe -
9.	Verlies van controle – Bestanden delen door gebruikers	**Maatregelen onderwijsinstellingen** Moedig periodieke evaluaties aan van welke documenten openbaar zijn gemaakt en implementeer procedures voor het handmatig verwijderen van openbare documenten na een bepaalde periode.
		Maatregelen Adobe Geef gebruikers duidelijk aan welke documenten openbaar worden gedeeld. **(Einde 2026)** Geef gebruikers prompts om hen eraan te herinneren welke documenten openbaar worden gedeeld. **(Einde 2026)** Geef gebruikers de mogelijkheid om op het moment van delen de tijd te beperken dat een document openbaar beschikbaar is.
10.	Verlies van controle – Toegankelijkheid projecten en bestanden door beheerders	**Maatregelen onderwijsinstellingen** Stel interne beleidsregels op waarin beheerders makers van werken op de hoogte stellen wanneer toegangsrechten zijn gewijzigd. Stel interne beleidsregels op waarin gebruikers worden geïnformeerd over wie binnen een organisatie toegang heeft tot hun bestanden op het moment dat deze worden aangemaakt.
		Maatregelen Adobe Breng projectmakers op de hoogte wanneer beheerders de toegangsrechten voor werken wijzigen.

		Breng gebruikers op de hoogte wanneer beheerders toegang krijgen tot bestanden en informeer gebruikers dat beheerders toegang hebben tot bestanden op het moment dat deze worden aangemaakt.
11.	Verlies van controle – De gebruiker is zich er niet van bewust dat functionaliteiten worden aangeboden door een online-dienst.	**Maatregelen onderwijsinstellingen** Beschrijf duidelijk de belangrijkste functionaliteiten (inclusief on-demand diensten).
		Maatregelen Adobe Voorzie gebruikers van documentatie en pop-ups die hen informeren welke functionaliteit in desktop-apps offline is en welke wordt gedeeld met Adobe.
12.	Verlies van controle – Gebruikers hebben beperkte mogelijkheden om documenten te verwijderen	**Maatregelen onderwijsinstellingen** Breng gebruikers op de hoogte van de huidige technische beperkingen.
		Maatregelen Adobe Biedt gebruikers de mogelijkheid om items in de Creative Cloud-webapplicatie op dezelfde manier te 'verwijderen' als in de desktopapplicatie **(Eind 2026).**
13.	Onevenredige verwerking van telemetriegegevens	**Maatregelen onderwijsinstellingen** Opt-out van optionele telemetrie wanneer en waar de optie beschikbaar is.
		Maatregelen Adobe Verkort de opslagperiode van alle telemetrie Verduidelijk welke telemetrie als verplicht wordt beschouwd en welke als optioneel Verwijder telemetrie wanneer gebruikersaccounts worden verwijderd Verzamel geen onnodige telemetrie en definieer duidelijk wat wel en wat niet noodzakelijk is Publiceer en update een lijst met telemetrie, verduidelijk welke verplicht is en waarom. Verduidelijk bovendien welke vormen van telemetrie worden verzameld wanneer de gebruiker hiervoor heeft gekozen. Verzamel geen telemetrie van desktopapplicaties wanneer deze door studenten worden gebruikt **(eind 2026)**.
14.	Verlies van controle – Content Credentials	**Maatregelen onderwijsinstellingen** -

		Maatregelen Adobe Informeer gebruikers over wat er wordt opgeslagen, hoe lang, voor welke doeleinden en wie toegang heeft tot die gegevens (voordat ze afbeeldingen genereren). Sla geen thumbnails op, in ieder geval niet voor niet-AI- of gedeeltelijk AI-content. Stel (niet onbeperkte) bewaartermijnen vast voor Content Credentials (met name voor gebruikers-ID's en thumbnails). Anonimiseer gegevens na een bepaalde periode of verwijder ze volledig. Breng Content Credentials volledig in overeenstemming met de Gedragscode voor AI Act artikel 50, wanneer deze in 2026 van kracht wordt.
15.	Onvermogen om rechten van betrokkenen uit te oefenen – onvolledige inzageverzoek-reacties Adobe	**Maatregelen onderwijsinstellingen** -
		Maatregelen Adobe Geef volledige gegevens in het inzageverzoek-antwoord. Geef volledige beschrijvingen/voldoende context zodat de betrokkene de teruggestuurde gegevens kan begrijpen (bijvoorbeeld uitleg over interne codes). Blijf duidelijke follow-upondersteuning bieden aan betrokkenen door eventuele verduidelijkende vragen over hun inzageverzoek-antwoorden te beantwoorden, zodat zij de verstrekte informatie begrijpen.
16.	Onvermogen om rechten van betrokkenen uit te oefenen – Beheerders niet in staat om inzageverzoeken na te leven	**Maatregelen onderwijsinstellingen** Creëer en onderhoud een proces speciaal voor het afhandelen van inzageverzoeken van gebruikers.
		Maatregelen Adobe Bied beheerders hulpmiddelen om inzageverzoeken van betrokkenen te beantwoorden. Geef duidelijke richtlijnen over de beperkingen van het systeem. Zorg ervoor dat er speciale ondersteuning van Adobe beschikbaar is om beheerders te helpen bij het navigeren en voltooien van inzageverzoeken.
17.	Onvermogen om rechten van betrokkenen uit te oefenen – Recht op	**Maatregelen onderwijsinstellingen** Maak duidelijke werkinstructies voor het verwijderen van gebruikers en het verwijderen van gebruikersassets.

	verwijdering/ beperking van opslag	Zorg ervoor dat gebruikers uit de lijst 'Actieve gebruikers' worden verwijderd nadat de gebruiker is verwijderd. Gebruik de Adobe Admin API's voor opslagbeheer om een bewaarbeleid voor inactieve gebruikers te configureren.
		Maatregelen Adobe Vereenvoudig het verwijderen van gebruikers door een manier te bieden om een gebruiker en al zijn directory's te verwijderen **(eind 2026)**. Werk de documentatie bij zodat deze overeenkomt met het verwijderingsproces in praktijk **(eind 2026)**. Informeer beheerders expliciet dat assets worden bewaard wanneer een gebruiker wordt verwijderd. Verwijder de assets van een gebruiker samen met het gebruikersaccount.

Inleiding

Deze DPIA is uitgevoerd in opdracht van SURF, de samenwerkingsorganisatie voor IT in het Nederlandse hoger onderwijs en onderzoek.

Gegevensbeschermingseffectbeoordeling

Op grond van de Algemene Verordening Gegevensbescherming (AVG) kan een organisatie onder bepaalde omstandigheden verplicht zijn om een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren, bijvoorbeeld wanneer het gaat om grootschalige verwerking van persoonsgegevens. De beoordeling is bedoeld om onder meer inzicht te geven in de specifieke verwerkingsactiviteiten, het inherente risico voor betrokkenen en de waarborgen die worden toegepast om deze risico's te beperken. Het doel van een DPIA is ervoor te zorgen dat alle risico's die aan het betreffende proces verbonden zijn in kaart worden gebracht en beoordeeld en dat er adequate waarborgen zijn geïmplementeerd om die risico's te beperken.

Een DPIA heette eerst PIA, *privacy impact assessment*. Volgens de AVG beoordeelt een DPIA de risico's voor de rechten en vrijheden van personen. Betrokkenen hebben een fundamenteel recht op bescherming van hun persoonsgegevens en enkele andere fundamentele vrijheden die door de verwerking van persoonsgegevens kunnen worden aangetast, zoals de vrijheid van meningsuiting.

Het recht op gegevensbescherming is dus ruimer dan het recht op privacy. Overweging 4 van de AVG luidt als volgt:

> "*Deze verordening eerbiedigt alle grondrechten alsook de vrijheden en beginselen die zijn erkend in het Handvest zoals dat in de Verdragen is verankerd, met name de eerbiediging van het privéleven en het familie- en gezinsleven, woning en communicatie, de bescherming van persoonsgegevens, de vrijheid van gedachte, geweten en godsdienst, de vrijheid van meningsuiting en van informatie, de vrijheid van ondernemerschap, het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, en het recht op culturele, godsdienstige en taalkundige verscheidenheid.*"

Paraplu-DPIA versus individuele DPIA's

In termen van de AVG is SURF **niet de verwerkingsverantwoordelijke** voor de verwerking van persoonsgegevens via het gebruik van Adobe Creative Cloud en Adobe Document Cloud. De verwerkingsverantwoordelijke is de individuele onderwijsinstelling die besluit om deze clouddienst te gebruiken. Als centrale onderhandelaar voor veel clouddiensten neemt SURF echter de verantwoordelijkheid op zich om de gegevensbeschermingsrisico's voor de eindgebruikers te beoordelen en ervoor te zorgen dat de gegevensverwerking in overeenstemming is met de AVG. Daarom geeft SURF opdracht tot paraplu-DPIA's om de onderwijsinstellingen te helpen bij het selecteren van een privacy conforme implementatie en om waar nodig hun eigen DPIA's uit te voeren. Alleen de organisaties zelf kunnen de specifieke risico's voor de gegevensbescherming beoordelen, die verband houden met de technische privacy-instellingen, de aard en omvang van de persoonsgegevens die zij verwerken en de kwetsbaarheid van de betrokkenen.

Deze paraplu-DPIA is bedoeld om de verschillende organisaties te helpen bij de DPIA die zij moeten uitvoeren wanneer zij Adobe Creative Cloud of Adobe Document Cloud implementeren, maar dit document kan niet de specifieke risicobeoordelingen die de verschillende organisaties zelf moeten uitvoeren vervangen.

Criteria EDPB
Overeenkomstig artikel 35 van de AVG is een DPIA verplicht als een voorgenomen gegevensverwerking een hoog risico inhoudt voor de betrokkenen van wie de persoonsgegevens worden verwerkt. De Nederlandse Autoriteit Persoonsgegevens (AP) heeft een lijst gepubliceerd met 17 soorten verwerkingen waarvoor in Nederland altijd een DPIA verplicht is.[2] Als een verwerking niet in deze lijst is opgenomen, moet een organisatie zelf beoordelen of de gegevensverwerking waarschijnlijk een hoog risico met zich meebrengt.

De Europese nationale toezichthoudende autoriteiten, verenigd in het Europees Comité voor gegevensbescherming (EDPB), hebben ook een lijst met negen criteria gepubliceerd.[6] Als vuistregel geldt dat als een gegevensverwerking aan twee van deze criteria voldoet, een DPIA vereist is.

De omstandigheden van de gegevensverwerking via Adobe Creative Cloud en Adobe Document Cloud voldoen aan drie van de negen criteria die door het EDPB zijn gedefinieerd:[7]

1) Gevoelige gegevens of gegevens van zeer persoonlijke aard (criterium 4). De EDPB legt uit: *"Sommige categorieën gegevens kunnen worden beschouwd als een verhoogd risico voor de rechten en vrijheden van personen. Deze persoonsgegevens worden als gevoelig beschouwd (zoals deze term algemeen wordt begrepen) omdat ze verband houden met huishoudelijke en privéactiviteiten (zoals elektronische communicatie waarvan de vertrouwelijkheid moet worden beschermd)."*
2) De verwerking heeft betrekking op gegevens van kwetsbare betrokkenen (criterium 7). Zowel werknemers als studenten van wie de persoonsgegevens worden verwerkt via Adobe Creative Cloud en Adobe Document Cloud, bevinden zich in een ongelijke machtsverhouding ten opzichte van de onderwijs- en onderzoeksinstellingen.
3) De verwerking omvat innovatief gebruik of de toepassing van nieuwe technologische of organisatorische oplossingen (criterium 8). In het geval van Adobe Creative Cloud valt de generatieve AI-functionaliteit die wordt aangeboden door de Firefly cloud AI-services onder dit criterium.

Reikwijdte van deze DPIA
Adobe Creative Cloud en Adobe Document Cloud zijn het onderwerp van deze DPIA.

Deze DPIA voor SURF omvat de online Admin Console waarmee de beheerder van een organisatie licenties en instellingen voor de organisatie kan beheren bij gebruik van zowel Adobe Creative Cloud als Adobe Document Cloud. Daarnaast analyseert de DPIA de gegevensbeschermingsrisico's van het gebruik van de creatieve applicaties Photoshop (fotobewerking) voor Windows en macOS. De analyse voor deze DPIA is uitgebreid met een beoordeling van de gegevensverwerking via deze diensten op macOS. Ten slotte heeft Privacy Company ook de generatieve AI-functionaliteit van Adobe getest op basis van Firefly cloud AI-services. Deze functionaliteiten zijn getest via de speciale Firefly-website, Photoshop en Adobe Express.

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

Tabel 2: Overzicht van diensten en platforms die onder de reikwijdte van deze DPIA vallen

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

Buiten de reikwijdte

Het toepassingsgebied van deze DPIA omvat niet het volgende:

- Acrobat AI Assistant[3]
- Functies voor het herschrijven en vertalen van tekst.
- Adobe Sign[4]
- Mobiele apps van Adobe
- Acrobat Microsoft-integraties (zoals Microsoft SharePoint en OneDrive, Microsoft Teams, Microsoft Word, Excel en PowerPoint).
- De 'oude' gebruikersinterface van de Acrobat-desktopapplicatie.[5]
- Bètaversies
- 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.
- Openbare webpagina's zoals het Adobe Community-forum (https://community.adobe.com/) en de Adobe Experience Cloud (https://experienceleague.adobe.com/).
- Aspecten van Adobe's gebruik van Amazon Web Services voor het hosten van applicaties en content.
- Adobe Firefly IP-vrijwaring. Adobe Firefly IP-vrijwaring is alleen beschikbaar in bepaalde productaanbiedingen en moet in het contract van de klant worden opgenomen om van toepassing te zijn. De huidige ETLA (Enterprise Terms Licensing Agreement) van SURF met Adobe bevat geen van de bovengenoemde productaanbiedingen en bevat dus geen dergelijke bepaling.[6]

[3] Acrobat AI Assistant kan samenvattingen maken van of vragen beantwoorden over PDF-documenten, op basis van natuurlijke taalopdrachten van gebruikers. Voor dit product is een aparte licentie vereist. Individuele gebruikers kunnen generatieve AI-functies uitschakelen in de productinstellingen en beheerders kunnen de toegang voor de hele organisatie intrekken door contact op te nemen met Adobe Customer Care. Zie: https://helpx.adobe.com/acrobat/using/disable-generative-ai.html, laatst bekeken op 6 januari 2025. Ook e-mail Adobe 17 januari 2025: "Deze functie is op veel locaties en in verschillende talen (Engels, Frans, Spaans, Portugees, Italiaans en Duits) beschikbaar in bètaversie. Hoewel AI Assistant door klanten in Nederland kan worden aangeschaft, is het nog niet beschikbaar in het Nederlands. Het is ook specifiek beperkt tot EDU-aanbiedingen (alleen beschikbaar voor HED-klanten in specifieke landen). Gebruikers moeten altijd een specifieke actie ondernemen om deze in te schakelen. Het is ook een advertentie, wat betekent dat het meer kost (hoewel er in bepaalde omstandigheden beperkte proefopties kunnen zijn). Als u Adobe Acrobat Pro koopt, is de AI een apart product. Er komt mogelijk in de toekomst een aanbod voor Enterprise-klanten (ETLA), maar dat is momenteel niet het geval en om te bevestigen dat AI Assistant ook niet standaard toegankelijk is voor Enterprise ETLA-gebruikers."

[4] Adobe Sign maakte aanvankelijk deel uit van de opdracht. Aangezien Adobe Sign een op zichzelf staand product is, zal voor Adobe Sign een afzonderlijke DPIA worden uitgevoerd.

[5] In september 2024 heeft Adobe een nieuwe Acrobat-gebruikersinterface beschikbaar gesteld voor alle gebruikers. Al onze tests zijn uitgevoerd met behulp van deze nieuwe gebruikersinterface. Zie 'Meer informatie over de nieuwe Acrobat', laatst bijgewerkt op 16 september 2024, URL: https://helpx.adobe.com/acrobat/learn-new-acrobat.html.

[6] E-mail Adobe 19 januari 2025.

Opmerking: Content Credentials[7] zijn momenteel nog een bètafunctie. Aangezien ze echter in Firefly zijn geïntegreerd, zijn ze nog steeds in beperkte mate opgenomen in deze DPIA. Adobe Stock is geïntegreerd in Firefly (als trainingsdata) en Adobe Stock is altijd aanwezig als dienst in de Adobe Creative Cloud (zij het in beperkte mate voor K-12-gebruikers). Hoewel Adobe Stock als zelfstandige dienst buiten het bereik viel, werd de toegang ertoe via de Creative Cloud getest.

Dit rapport is geen specifieke KIA[8], een kinderenrechten impact assessment, maar bevat speciale hoofdstukken die zich op kinderen richten. Het bevat ook geen afzonderlijke IAMA, een impact assessment mensenrechten en algoritmes bij het gebruik van ingebouwde AI-diensten. Hiervoor heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een apart model ontwikkeld.

Methodologie
Deze DPIA is gebaseerd op een uitgebreide onderzoeksmethodologie. Privacy Company combineerde een juridische feitenonderzoekstrategie met een technisch onderzoek van de gegevens die worden verwerkt door het gebruik van Adobe Creative Cloud en Adobe Document Cloud.

Juridisch feitenonderzoek
Privacy Company heeft de door SURF en Adobe verstrekte informatie en openbaar beschikbare informatie bestudeerd. Daarnaast hebben SURF, Adobe en Privacy Company een workshop gehouden met het Trust & Safety-team van Adobe over kinderveiligheid.

Technisch onderzoek
Het technische deel van het onderzoek omvat inspectie van de instellingen die beschikbaar zijn voor beheerders en eindgebruikers en het uitvoeren van testscenario's die bedoeld zijn om het gangbare gebruik van de diensten weer te geven.

Testscenario's
Om ervoor te zorgen dat alle bevindingen kunnen worden gereproduceerd, heeft Privacy Company gescripte testscenario's uitgevoerd. Deze scenario's worden beschreven in paragraaf 2.3 en in de technische bijlage. Deze tests hebben betrekking op typische gebruikssituaties voor leerlingen en docenten op webgebaseerde Adobe Creative Cloud-toepassingen, Mac-desktop Adobe Creative Cloud-toepassingen en Windows-desktop Adobe Creative Cloud-toepassingen. Privacy op School[9] heeft feedback/input gegeven voor de testscenario's. Privacy op School heeft informatie verstrekt over het reguliere (beoogde) gebruik binnen het basis- en voortgezet onderwijs en in mindere mate over het onbedoelde of oneigenlijke gebruik van Adobe-producten.

Technische tests
Privacy Company gebruikte een combinatie van de tools Mitmproxy en Wireshark om het webverkeer tijdens de gescripte testscenario's te onderscheppen. Met deze tools kan Privacy Company cookies en andere soorten gegevens observeren die vanaf de testapparaten naar externe servers worden verzonden. Een overzicht van de testomgeving is te vinden in tabel 3.

[7] Adobe, 'Content Credentials', laatst bijgewerkt op 14 oktober 2024, URL: https://helpx.adobe.com/creative-cloud/help/content-credentials.html.
[8] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, KIA Template, URL: https://www.digitaleoverheid.nl/document/kia-invuldocument/.
[9] Privacy op School is een Nederlandse organisatie met het doel om alle onderwijsorganisaties te helpen en ondersteunen met privacy- en informatiebeveiligingsvraagstukken URL: https://www.privacyopschool.nl/.

Tabel 3: Overzicht van technische tools die bij het testen zijn gebruikt

Tool	Versie	Beschrijving van het gebruik
Windows-laptop	Processor: 11th Gen Intel(R) Core(TM) i7-11800H @ 2.30 GHz 2.30 GHz, x64-based processor Microsoft Windows 11 Pro	Gebruikt bij het onderscheppen van verkeer en voor het uitvoeren van Adobe-toepassingen.
Mac-laptop en Google Chrome-browser	macOS 10.15.7 Apple M3 Pro processor Google Chrome[10] browser version 129	Gebruikt bij het onderscheppen van verkeer en voor het uitvoeren van Adobe-applicaties op desktop en web.
Mitmproxy	Versie 10.2.2[11]	Gebruikt om webverkeer van browsers en Adobe-toepassingen te onderscheppen.
Wireshark	Versie 4.0.7[12]	Gebruikt om webverkeer van browsers en Adobe-applicaties te onderscheppen.
Adobe Creative Cloud Desktop-applicatie[13]	Versie 6.4.0.361	Gebruikt om de testscenario's uit te voeren.

Opzet van deze DPIA
Deze DPIA volgt de structuur van het Model Gegevensbeschermingseffectbeoordeling Rijksdienst (DPIA). Dit model maakt gebruik van een structuur met vier hoofdonderdelen.

A. Beschrijving van de feitelijke gegevensverwerking
B. Beoordeling van de rechtmatigheid van de gegevensverwerking
C. Beoordeling van de risico's voor betrokkenen
D. Beschrijving van risicobeperkende maatregelen

Deel A geeft een algemene, gedetailleerde uitleg van de verwerkingsactiviteiten via Adobe Creative Cloud en Adobe Document Cloud op basis van de geteste configuratie. Dit begint met een beschrijving van de manier waarop de gegevens worden verzameld en verwerkt en beschrijft de categorieën persoonsgegevens en betrokkenen die door de verwerking kunnen worden beïnvloed, de doeleinden van de gegevensverwerking, de verschillende rollen van de partijen, de verschillende belangen die met deze verwerking verband houden, de locaties waar de gegevens worden opgeslagen en de bewaartermijnen. Voor dit deel zijn het contract van SURF met Adobe en andere juridische documentatie beoordeeld. Daarnaast zijn testscenario's uitgevoerd, zijn inzageverzoeken van betrokkenen ingediend en is aanvullende informatie opgevraagd bij Adobe.

[10] Google, Chrome, URL: https://www.google.com/chrome/, laatst bekeken op 4 februari 2025.
[11] Mitmproxy, HTTPS proxy., URL: https://mitmproxy.org, laatst bekeken op 20 december 2024.
[12] Wireshark, network protocol analyser, URL: https://wireshark.org/, laatst bekeken op 20 december 2024.
[13] Adobe Creative Cloud, URL: https://creativecloud.adobe.com/, laatst bekeken op 20 december 2024.

Deel B bevat een beoordeling door Privacy Company van de rechtmatigheid van deze gegevensverwerkingen via Adobe Creative Cloud en Adobe Document Cloud. Privacy Company heeft de naleving van de belangrijkste beginselen van gegevensverwerking beoordeeld, te beginnen met de rechtsgrondslag en met inbegrip van transparantie, gegevensminimalisatie, doelbinding en evenredigheid. In dit deel wordt ook afzonderlijk ingegaan op de rechtmatigheid van eventuele doorgiften van persoonsgegevens naar landen buiten de EER, en op de wijze waarop de rechten van de betrokkenen worden geëerbiedigd.

Deel C beoordeelt de risico's voor de rechten en vrijheden van de betrokkenen die voortvloeien uit de verwerkingsactiviteiten als gevolg van het gebruik van Adobe Creative Cloud en Adobe Document Cloud in deel A van deze DPIA. Het noemt specifieke risico's die voortvloeien uit deze verwerkingsactiviteiten en heeft tot doel zowel de waarschijnlijkheid dat deze risico's zich voordoen als de ernst van de gevolgen voor de rechten en vrijheden van de betrokkenen indien de risico's zich voordoen specifiek te bepalen. Deel C bevat ook een analyse van de ernst van elk risico, op basis van de waarschijnlijkheid dat het zich voordoet en de mogelijke gevolgen voor de rechten en vrijheden van de betrokkenen.

Ten slotte worden in **deel D** concrete maatregelen beschreven die door Adobe of de onderwijsinstellingen kunnen worden genomen om de in deel C geïdentificeerde risico's te beperken. Deze maatregelen kunnen de kans dat deze risico's zich voordoen, de mogelijke gevolgen ervan, of beide verminderen. Deel D bevat ook een beoordeling van eventuele resterende risico's die verband houden met het gebruik van Adobe Creative Cloud en Adobe Document Cloud, voor zover deze niet door de onderwijsinstellingen kunnen worden beperkt door de voorgestelde maatregelen toe te passen.

Tijdlijn van deze DPIA
Deze tijdlijn is gebaseerd op de correspondentie tussen Privacy Company, SURF en Adobe gedurende het project. Hoewel het tijdschema feitelijk is, geeft het geen beeld van de directe communicatie of uitwisselingen die mogelijk hebben plaatsgevonden tussen SURF en Adobe.

Er hebben verschillende vroege vergaderingen en verkennende gesprekken plaatsgevonden voordat het formele onderzoek begon. Voor de duidelijkheid: deze tijdlijn begint op het moment dat Privacy Company met de technische tests is begonnen. De technische tests vonden plaats in week 37, 38 en 39 van 2024. De inzageverzoeken werden op 30 september 2024 ingediend en Adobe bevestigde de ontvangst van de inzageverzoeken op 3 oktober 2024. Adobe gaf op 30 oktober 2024 een eerste reactie op de verzoeken, gevolgd door een uitgebreidere reactie met aanvullende informatie op 13 december 2024. De tweede reactie was een meer gedetailleerde teruggave van gegevens, waarvoor volgens Adobe extra tijd nodig was.

Het eerste concept van deel A van dit rapport is op 7 februari 2025 voltooid. Deel A geeft een momentopname weer van Adobe-software en -diensten voordat Adobe reageerde op de opmerkingen van SURF met verduidelijkingen, correcties, wijzigingen of geplande maatregelen. Waar Adobe dergelijke werkzaamheden heeft uitgevoerd, wordt dit door SURF aan het einde van de beschrijvingen in deel A vermeld. De beschrijvingen in deel A moeten dan ook niet worden opgevat als de huidige stand van zaken op 12 februari 2026, maar eerder als een eerste analyse, voorafgaand aan de samenwerking tussen Adobe en SURF. Waar werkzaamheden zijn uitgevoerd of kwesties zijn verduidelijkt, heeft SURF dit aan het einde van de paragraaf vermeld om het uitgangspunt en de huidige stand van zaken weer te geven.

Op 14 mei 2025 werd het volledige concept van de DPIA voltooid. Gedurende 2025 werden verschillende rondes van vragen en feedback over het rapport gehouden, waaronder verduidelijking van kwesties en het zoeken naar oplossingen. Op 22 september 2025 hadden

Adobe, SURF en Privacy Company een bijeenkomst om de Trust and Safety-maatregelen van Adobe te bespreken, waaronder de scanmethoden en -technieken voor CSAM.

Het definitieve rapport werd op 12 februari 2026 voltooid.