Lokale DPIA

Google Workspace for Education [en

ChromeOS op beheerde Chromebooks]

lokale DPIA uit te voeren door schoolbesturen, gebaseerd op landelijke DPIA, DTIA en verificatie door SIVON en SURF

Versie 3.0 (24 juni 2024)

COLOFON

DPIA en DTIA uitgevoerd door	Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A. (SIVON) www.sivon.nl info@sivon.nl en coöperatie SURF www.surf.nl info@surf.nl
Betrokkenen bij uitvoering DPIA	Privacy Company (Den Haag) www.privacycompany.nl GreenbergTraurig (GT Law) Amsterdam www.gtlaw.com
Auteurs lokale DPIA	Versie 1.0: Ymkje Koster (Kennisnet) en Job Vos (SIVON) Versie 2.0: Hans-Peter Ligthart en Job Vos (SIVON) Versie 3.0: Hans-Peter Ligthart en Job Vos (SIVON)
Versie	1.0: 5 augustus 2021 2.0: update 13 juli 2023 3.0: update 24 juni 2024

Bij deze DPIA is gebruik gemaakt van de door Privacy Company uitgevoerde DPIA en DTIA op Google Workspace for Eduation, de Model DPIA van SIVON en de Model DPIA Rijksoverheid versie 2.0.

SIVON en Kennisnet worden gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW). Deze publicatie is tot stand gekomen in samenwerking met SURF en SIVON. SIVON en Kennisnet bevorderen samenwerking tussen schoolbesturen op het gebied van ict-infrastructuur, leermiddelen en leeromgevingen en informatiebeveiliging en privacy (IBP). SIVON helpt scholen bij het realiseren en doorontwikkelen van veilig en toekomstbestendig digitaal onderwijs, nu en in de toekomst; zij adviseert, ontzorgt en behartigt de belangen van scholen, zodat die zich kunnen richten op hun primaire taak: het verzorgen van het allerbeste onderwijs.

Inhoudsopgave

1. Inleiding

1.1 Algemeen

In 2021 is er een privacyonderzoek uitgevoerd op Workspace for Education (in 2021 nog G Suite for Education genoemd). Uit deze *data protection impact assessment* (DPIA) bleek dat er hoge privacyrisico's kleefden aan het gebruik van Google Workspace for Education. Deze software - die onder meer de programma's als Google Classroom, Google Docs, en Google Meet bevat - wordt ook op de scholen van [NAAM ONDERWIJSINSTELLING] gebruikt.

SIVON en SURF, coöperaties van en voor onderwijs- en onderzoeksinstellingen in Nederland, hebben naar aanleiding van het onderzoek in 2021 afspraken gemaakt[1] met Google om de geconstateerde privacyrisico's te verminderen. Google is de afspraak nagekomen en heeft de nodige maatregelen genomen en wijzigingen doorgevoerd in de software. Deze zijn medio 2023 door SIVON en SURF en de door hen ingeschakelde externe privacyexperts gecontroleerd. Deze uitkomsten zijn opgenomen in het "*Verification report Google remediation measures Workspace for Education*" van Privacy Company (dd 15 juni 2023). Op basis van de DPIA is in schooljaar 2023/2024 een *Data Transfer Impact Assessment (DTIA)* uitgevoerd en zijn er vijf nieuwe privacy-risico's geconstateerd die na overleg met opgelost.

Verder is het gebruik van ChromeOS en Chromebrowser op door de onderwijsinstellingbeheerde chromebooks onderzocht. Hierover zijn in 2023[2] afspraken gemaakt met Google om de daarbij geconstateerde privacy-risico's te beperken.

In 2024 hebben SURF en SIVON het overleg met Google afgerond en zijn de door Google genomen maatregelen geverifieerd. Dat heeft geresulteerd in vier (eind)rapporten:

1. Public version Updated Verification Report Workspace for Education – 17 May 2024
2. Public version DTIA Google Meet (Workspace for Education) – 11 April 2024
3. Public version New findings review Google Workspace for Education – 16 May 2024
4. Public version Verification Report Processor version Google Chrome for Education – 7 March 2024.

SIVON en SURF concluderen[3] na grondig onderzoek dat scholen Google Workspace for Education en ChromeOS en Chromebrowser op beheerde chromebooks **kunnen blijven gebruiken**. Voorwaarde hierbij is dat scholen de technische en organisatorische maatregelen die SURF en SIVON adviseren te nemen, opvolgen. Daarnaast moet iedere onderwijsinstelling zelf in een (lokale) DPIA de uitkomsten van het onderzoek van SURF en SIVON bevestigen en vaststellen dat er geen aanvullende risico's zijn.

Dit rapport helpt onderwijsinstellingen om in een eigen DPIA (door SIVON lokale DPIA genoemd) de uitkomsten van de onderzoeken van SURF en SIVON te bevestigen.

[1] https://sivon.nl/2021/07/akkoord-onderwijs-met-google-over-privacyrisicos/
[2] SIVON, SURF en Google bereiken overeenkomst Terms of Service Google Chrome - SIVON
[3] https://sivon.nl/2023/07/privacyrisicos-uit-dpia-van-2021-google-workspace-for-education-voldoende-opgelost/

1.2 Verplichte uitvoering DPIA

Om vast te stellen of de gegevens van leerlingen en medewerkers (persoonsgegevens) in een applicatie, software of ict-middel veilig en verantwoord gebruikt worden, is volgens de AVG verplicht om een Data Protection Impact Assessment (DPIA) uit te voeren. In de AVG wordt dit een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Een DPIA wordt uitgevoerd op een proces, applicatie of verwerking van persoonsgegevens. Meestal gaat het om een applicatie van een leverancier (verwerker). De DPIA wordt uitgevoerd volgens de eisen van artikel 35 van de AVG.

Een DPIA wordt uitgevoerd door een verwerkingverantwoordelijke. In het onderwijs is dat het onderwijsinstelling (bevoegd gezag).

Met een DPIA wordt beoordeeld wat de risico's en (mogelijke) gevolgen zijn van het gebruik van de applicatie voor de bescherming van de persoonsgegevens van de leerlingen, hun ouders en medewerkers. Er wordt vastgesteld wordt of het gebruik van persoonsgegevens (verwerking) een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen. Als de privacyrisico's (te) hoog zijn, moet er worden gezocht naar maatregelen om deze risico's te beperken. Dit worden mitigerende maatregelen genoemd. Als de hoge risico's niet weggenomen kunnen worden, dan mag volgens de AVG deze verwerking (gebruik applicatie) niet worden uitgevoerd of voortgezet.

De uitkomst van de DPIA is o.a. een rapportage met daarin een overzicht van geclassificeerde risico's voor de rechten en vrijheden van betrokkenen. In het rapport staan ook de nodige mitigerende maatregelen benoemd. De verwerkingsverantwoordelijke stelt uiteindelijke de DPIA vast, hiermee wordt vastgesteld welke maatregelen nog moeten worden uitgevoerd en dat het onderwijsinstelling de resterende vastgestelde risico's accepteert.

Een DPIA is verplicht als de verwerking van persoonsgegevens - gelet op de aard, de omvang, de context en de doeleinden van die verwerking - waarschijnlijk een hoog risico inhoudt voor de 'rechten en vrijheden' (privacy) van leerlingen en medewerkers. Ook is het mogelijk dat het uitvoeren van een DPIA verplicht is volgens de regels van de privacy toezichthouder Autoriteit Persoonsgegevens (AP) die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van aan DPIA verplicht is[4].

Voor het onderwijs betekent dit dat een DPIA altijd verplicht is op tenminste het leerlingvolg- en/of -administratiesysteem (LVS/LAS), personeelsadministratiesysteem en breed ingezette applicaties met digitaal leermateriaal.

De uitvoering van een DPIA op Google Workspace for Education en/of ChromeOS en Chromebrowser is verplicht omdat er uit het onderzoek is gebleken van hoge privacy-risico's die na maatregelen zijn gemitigeerd.

1.3 Centrale versus lokale DPIA

Met de onderhandelingen en afspraken met Google en het gepubliceerde verificatierapport, zijn grote en goede stappen gezet om privacyrisico's van het gebruik van Google Workspace for Education door het Nederlandse onderwijs weg te nemen. Maar de Europese privacywetgeving Algemene Verordening Gegevensbescherming (AVG) eist dat organisaties die zelf (eind)verantwoordelijk zijn voor gegevensbescherming, zelf een privacyonderzoek uitvoeren. De privacytoezichthouder Autoriteit Persoonsgegevens onderschrijft deze verplichting:

Leerlingen en studenten hebben een grondwettelijk recht op bescherming van hun persoonsgegevens en dienen te worden beschermd tegen schendingen van dat grondrecht. Zeker kinderen hebben recht op specifieke bescherming bij de verwerking van hun persoonsgegevens. Nu individuele onderwijsinstellingen de keuze maken voor de inzet van een bepaald product, softwarepakket of clouddienst, dienen deze onderwijsinstellingen vast te stellen dat deze keuze de grondwettelijke rechten van kinderen niet schaden. Onderwijsinstellingen dienen daartoe in hun hoedanigheid als verwerkingsverantwoordelijke onder de Algemene verordening gegevensbescherming (AVG) zelf een DPIA uit te voeren en de gedocumenteerde afweging te maken of de inzet van de Google producten veilig kan plaatsvinden.. [4]

Onderwijsinstellingen moeten dus zelf besluiten of zij het gebruik van Google Workspace for Education willen en kunnen voortzetten (of starten) op basis van het privacyonderzoek van SURF en SIVON. Onderwijsinstellingen moeten als verwerkingsverantwoordelijke zelf een risicoafweging moeten maken en vaststellen. Hierbij kan en mag gebruik worden gemaakt van de uitkomsten van het landelijk onderzoek van SURF en SIVON. Deze DPIA wordt centrale DPIA genoemd.

Daarnaast moeten scholen nagaan of er bij het gebruik van Google Workspace for Education en ChromeOS op beheerde chromebooks op de eigen scholen nog andere privacyrisico's bestaan die moeten worden weggenomen. Deze uitkomsten komen in de eigen DPIA, die lokale DPIA wordt genoemd.

De methodiek die bij de lokale DPIA wordt gevolgd, is beschreven door de Britse privacy-toezichthouder ICO[5] om risico's te classificeren. Hierbij wordt een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade).

1.4 Uitvoering lokale DPIA

Bij de lokale DPIA bij [NAAM ONDERWIJSINSTELLING] zijn de volgende medewerkers betrokken:

- Bijvoorbeeld [ict-afdeling]
- [lid IBP-team]
- [privacy officer]
- [security officer]
- [key-user/gebruiker]
- [vertegenwoordiging betrokkenen]

De lokale DPIA is uitgevoerd in de periode [periode].

[NAAM ONDERWIJSINSTELLING] maakt gebruik van [Google Workspace for Education Fundamental/Standard/Plus] [en ChromeOS en Chromebrowser op beheerde chromebooks] voor [leerlingen] [en medewerkers].

[4] https://autoriteitpersoonsgegevens.nl/uploads/imported/brief_ap_privacy_in_het_onderwijs_bij_google-producten.pdf

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how10

Van deze lokale DPIA maken de volgende documenten integral onderdeel uit:

1. Public version Updated Verification Report Workspace for Education – 17 May 2024
2. Public version DTIA Google Meet (Workspace for Education) – 11 April 2024
3. Public version New findings review Google Workspace for Education – 16 May 2024
4. Public version Verification Report Processor version Google Chrome for Education – 7 March 2024
5. Technische handleiding voor Google Workspace for Education v3.0
6. Handleiding ChromeOS en Chrome-browser 2024.

1.5 Leeswijzer en gebruiksinstructie lokale DPIA

De onderwijsinstelling kan deze model lokale DPIA gebruiken en zelf invullen. In paragraaf 1.4 vult de onderwijsinstelling de informatie in over de uitgevoerde lokale DPIA.

In hoofdstuk 2 (Gegevensverwerkingsanalyse) stelt het bestuur van de onderwijsinstelling vast voor welke doelen de producten Google Workspace for Education en/of ChromeOS worden gebruikt.

In hoofdstuk 3 (Risicoanalyse) worden de landelijk gevonden privacy-risico's besproken en beoordeeld. Hierbij kunnen eventuele eigen aanvullende risico's en maatregelen door de onderwijsinstelling worden toegevoegd.

In hoofdstuk 4 (Eindconclusie) wordt de conclusie getrokken of de privacy-risico's op basis van de lokale DPIA voldoende zijn beperkt, inclusief de afwegingen en genomen en te nemen maatregelen. In hoofdstuk 5 stelt het bestuur (bevoegd gezag) de uitkomsten van de DPIA zelf vast in een bestuursverklaring.

In bijlage 1 en 2 is een overzicht opgenomen van de te nemen technische maatregelen.

In dit model zijn de onderdelen die door de onderwijsinstelling moeten worden ingevuld, geel gearceerd. Er wordt uitgegaan van het gebruik van Google Workspace for Education. Een groot aantal onderwijsinstellingen gebruikt daarnaast ook ChromeOS en Chrome-browser op beheerde chromebooks. Per onderdeel moet daarom bij de geel gearceerde teksten worden gekozen om de tekst aan te passen als de onderwijsinstelling ChromeOS al dan niet gebruikt.

2. Gegevensverwerkingsanalyse

In dit onderdeel stelt het bestuur van de onderwijsinstelling vast op welke wijze Google Workspace for Education en/of ChromeOS en Chromebrowser op beheerde chromebooks wordt gebruikt binnen de eigen organisatie. De landelijk uitgevoerde DPIA en DTIA richten zich op het gebruik van de Google-producten in het onderwijs als officepakket, in aanvulling op reeds bestaande ict-infrastructuur, ict-middelen en gebruikte applicaties zoals het leerling- en personeelsadministratiesysteem.

2.1 Betrokkenen

De centrale DPIA, alsmede de lokale DPIA, onderzoeken de gevolgen voor de rechten en vrijheden van betrokkenen door de verwerking van hun persoonsgegevens in Google Workspace for Eduation - na toepassing van risico-mitigerende maatregelen. De betrokkenen zijn leerlingen en/of medewerkers van de onderwijsinstelling.

Bij leerlingen in het primair en voortgezet onderwijs zijn er specifieke risico's voor minderjarige gebruikers van Google Workspace for Education-services van toepassing. In het Update DPIA Report uit 2021[6] wordt hier een beschrijving van gegeven (vanaf pagina 31). Bij minderjarigen in Nederland gaat het in het kader van de AVG om kinderen jonger dan 16 jaar. De Nederlandse privacytoezichthouder Autoriteit Persoonsgegevens (AP) heeft de persoonsgegevens van deze minderjarigen gekwalificeerd als ‘gevoelige persoonsgegevens’. Van deze leerlingen kan niet worden verwacht dat ze zelfstandig privacymaatregelen treffen en ze hebben ook niet de mogelijkheid om toestemming te geven voor het gebruik van schoolfaciliteiten of dit te weigeren (dat is aan hun wettelijke vertegenwoordigers/ouders/verzorgers). De AP vereist dat onderwijsinstellingen in de DPIA specifiek het risico voor minderjarige leerlingen meewegen.

De betrokkenen zijn [leerlingen en/of medewerkers]. [Beschrijving gebruik door betrokkenen.]

Bij leerlingen gaat het om leeftijdsgroepen:

	Leeftijdscategorie	Bijzondere risico’s
☐	6 – 9 jaar	In deze leeftijdsgroep leren kinderen lezen en schrijven en beginnen ze ICT te gebruiken. Jongere kinderen (4-6) kunnen al in aanraking komen met het Google-ecosysteem wanneer de leerkracht YouTube-filmpjes op het whiteboard in de klas. Zowel thuis als op onderwijsinstelling kijken kinderen veel YouTube-clips, zelfs op zeer jonge leeftijd. Het gebruik richt zich klikken op bekende en aangeboden picto’s en plaatjes omdat niet alle gebruikers in staat zijn goed te lezen en begrijpen waarop ze klikken.
☐	9 – 12 jaar	Deze leeftijdsgroep is gedefinieerd als een aparte categorie, omdat kinderen op deze leeftijd zelf beginnen met het gebruik van mobiele telefoons. Ze delen hun leven en wereld met elkaar en met de buitenwereld zonder zich bewust te zijn van de gevaren/risico's. Op deze leeftijd loggen kinderen in en klikken ze weg, meestal zonder te weten wat ze aan het doen zijn. Ze besteden geen aandacht aan het soort omgeving waarin ze werken (educatief of commercieel).

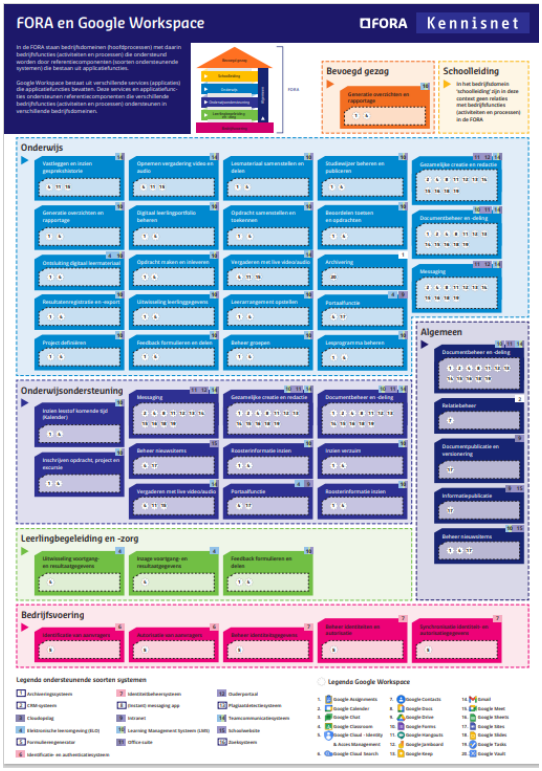
[6] https://sivon.nl/wp-content/uploads/2022/07/Update-DPIA-report-Google-Workspace-for-Education-2-augustus-2021.pdf

☐	12-16 jaar	Op 12-jarige leeftijd gaan kinderen naar scholen voor voortgezet onderwijs. Het gebruik van ICT is normaal. Ze hebben meestal hun eigen mobiele smartphones en koppelen hun schoolaccounts aan hun privéaccounts. Op deze leeftijd lezen kinderen over het algemeen niet zorgvuldig de voorwaarden en uitleg over privacykeuzes. Het gebruik is doelgericht om door te gaan: ze klikken op elke website gewoon Ja op elke groene knop, ongeacht de gevolgen van de standaardinstellingen. Tegelijkertijd is de druk van leeftijdsgenoten erg groot, om allerlei sociale media te gebruiken met zeer privacyschendende kenmerken.

Toelichting: Google heeft een speciale K-12 instelling ontwikkeld in Google Workspace for Education, bedoeld voor leerlingen tot 18 jaar. Door zichzelf als K-12 aan te merken, profiteren scholen en universiteiten van de meest privacyvriendelijke instellingen in Google Workspace for Education. Google heeft bevestigd dat het geen leeftijdscontrole toepast: universiteiten en instellingen voor beroepsonderwijs kunnen, en worden aanbevolen, ook de K-12 instellingen te kiezen om te profiteren van deze privacyvriendelijke instellingen. Maar K-12 kiezen is niet genoeg: alleen de betaalde versies van Workspace for Education bieden de nodige centraal afdwingbare privacybescherming die tegemoetkomt aan de specifieke bijzondere privacy-risico's voor minderjarigen.

2.2 Processen en gebruik Google Workspace for Education

De basis voor deze analyse zijn procesbeschrijvingen, waarbij gebruik is gemaakt van de bedrijfsfuncties die zijn beschreven in de FORA[7].



[7] 8733_Figuur_Toepassingen_Google_Workspace-FORA_FASE_2_-_2022_01.pdf (wikixl.nl)

Google Workspace for Education wordt gebruikt voor/als:
Archiveringssysteem, CRM-systeem, Cloudopslag, Elektronische leeromgeving (ELO), Formulierengenerator, Identificatie- en authenticatiesysteem, Identiteitbeheersysteem, (Instant) messaging app, Intranet, Learning Management Systeem (LMS), Office suite, Ouderportaal, Plagiaatdetectiesysteem, Teamcommunicatiesysteem (waaronder videoconferencing en chat), Schoolwebsite, Zoeksysteem
De volgende onderdelen van Google Worspace for Education worden gebruikt:

1. Google Assignments
2. Google Calender
3. Google Chat
4. Google Classroom
5. Google Cloud - Identity & Acces Management
6. Google Cloud Search
7. Google Contacts
8. Google Docs
9. Google Drive
10. Google Forms
11. Google Hangouts
12. Google Jamboard
13. Google Keep
14. Gmail
15. Google Meet
16. Google Sheets
17. Google Sites
18. Google Slides
19. Google Tasks
20. Google Vault

2.3 Doeleinden verwerkingen persoonsgegevens

In onderstaande tabel zijn de bedrijfsfuncties uit de FORA overgenomen. De bedrijfsfuncties kunnen ook worden gezien als doeleinden, zoals bedoeld in de AVG. Geef per bedrijfsfunctie/doeleinde aan of ze van toepassing zijn binnen uw onderwijsinstelling.

Hoofdbedrijfsfunctie	Bedrijfsfunctie/doeleinde	Kruis aan indien van toepassing op onderwijsinstelling
Samenwerken en communiceren medewerkers en extern	Documentbeheer en -deling	☐
	Communicatie van nieuws en updates	☐
	Gerichte communicatie	☐
	Beheer van relaties en externe betrekkingen	☐
	Beheer van referentie-informatie (bijv. standaardlijsten met codes voor afdelingen, locaties, kostenplaatsen etc.)	☐
Samenwerken en communiceren ouders	Oudercommunicatie klasbreed	☐
	Oudercommunicatie leerlingspecifiek	☐
Samenwerken en communiceren leerlingen	Leerlingen informeren over logistieke zaken	☐
	Inschrijving projecten en excursies	☐
	Ondersteuning samenwerken in leerlingprojecten	☐

Onderwijs-ondersteuning: instroom, doorstroom, uitstroom	Groepen en klassenbeheer	☐
Onderwijsvoorbereiding	Opleidingontwikkeling	☐
	Materiaalontwikkeling	☐
	Planning en roostering	☐
Onderwijsuitvoering	Lesuitvoering	☐
	(Toegang tot) aanbod leermateriaal	☐
	Toetsafname	☐
Onderwijsevaluatie	Beoordeling	☐
	Resultatenregistratie	☐
	Terugkoppeling feedback	☐
Passend onderwijs	Voortgang- en resultaatweergave	☐
Ict-ondersteuning	Authenticatie en autorisatie	☐
	Beheer identiteiten	☐
	Ict-servicemanagement (device management)	☐
Informatiebeveiliging en privacy	Realisatie beveiligingsmaatregelen (logging en monitoring)	☐
Realisatie en onderhoud van digitale toegankelijkheid	Het ervoor zorgen dat applicaties goed toegankelijk zijn op verschillende type devices.	☐
Andere bedrijfsfuncties/ doeleinden, namelijk:		
	…	☐
	…	☐

Bij een ander dan hiervoor beschreven gebruik, zijn er mogelijk privacy-risico's van toepassing die niet onderzocht zijn in het kader van de landelijke DPIA en DTIA.

2.4 Persoonsgegevens

Voor het in gebruik nemen van een account in Google Workspace for Education en ChromeOS en Chromebrowser op beheerde chromebooks, is maar een beperkte set gegevens van betrokkene (leerling, medewerker) nodig: voornaam, achternaam, wachtwoord en school-e-mailadres. Het is hierbij niet noodzakelijk om de echte voor- en achternaam van een betrokkene te gebruiken. Het advies is om in het e-mailadres geen naam op te nemen.

Ten aanzien van het gebruik van ChromeOS en Chromebrowser op beheerde chromebooks, geldt dat hierbij gebruik wordt gemaakt van device- en identitymanagement binnen Google Workspace for Education. Er zijn geen aanvullende gegevens vereist. Voor het beheer van chromebooks is wel een specifieke licentie nodig (voor de levensduur van het device): Chrome Education Upgrade.

Wanneer een betrokkene gebruik maakt van de services binnen Google Workspace for Education worden gebruiksgegevens (metadata) gegenereerd. Door gebruik te maken van de door SIVON en SURF met Google onderhandelde contracten en het toepassen van de technische maatregelen zoals beschreven in de *Handleiding technische maatregelen (v3.0 - 2024)* is de verzameling en verwerking van deze gebruiksgegevens tot een noodzakelijk minimum beperkt.

Als uw onderwijsinstelling nog andere persoonsgegevens verwerkt binnen Google Workspace for Education (bijvoorbeeld persoonsgegevens die worden vastgelegd in Google docs, Spreadsheet of Gmail) dan geeft u dat hieronder aan. In verband met het vereiste van dataminimalisatie motiveert u daarbij waarom deze persoonsgegevens worden verwerkt.

Geef hieronder per soort betrokkene aan welke persoonsgegevens binnen Google Workspace door uw onderwijsinstelling worden verwerkt.

Persoonsgegevens in Google Workspace for Education		
Betrokkene(n) (leerling, medewerkers, ouders, andere betrokkene)	**Verwerkte persoonsgegevens**	**Motivatie**
Leerling, medewerker	(Fictieve) voornaam	Deze gegevens zijn nodig voor het aanmaken van een account in Google Workspace for Education
	(Fictieve) achternaam	
	Wachtwoord	
	E-mailadres (school)	
Leerling, medewerker	Diagnostische gegevens, zoals log- en monitoringsgegevens, metadata	*Zie rapportages landelijke DPIA, DTIA Google Workspace for Education en Verification Report ChromeOS*
	IP-adres	
	Persoonsgegevens gebruikers (*Customer data*) in bestanden	
…	Andere persoonsgegevens, namelijk: … … …	…

2.5 Beoordeling van de rechtmatigheid

Geef hieronder per hoofdbedrijfsfunctie die voor u van toepassing is aan:

- wat de wettelijke grondslag is van de verwerkingen in dat proces.
- of voldaan is aan het vereiste van dataminimalisatie (worden er niet meer persoonsgegevens verwerkt dan noodzakelijk). Hou hierbij ook rekening met de specifieke risico's en maatregelen als het gaat om het verwerken van persoonsgegevens van kinderen jonger dan 16 jaar in Google Workspace for Education.

- of voldaan is aan het vereiste van transparantie. Zijn de betrokkenen afdoende geïnformeerd over de verwerking van hun persoonsgegevens en de rechten die ze daarbij kunnen uitoefenen?

*Als u Google Workspace for Education **niet** gebruikt voor één of meer van de genoemde hoofdbedrijfsfuncties (zie daarvoor de tabel in paragraaf 2.2), dan verwijdert u hieronder de betreffende tabel(len).*

Hoofdbedrijfsfunctie	**Beoordeling rechtmatigheid**	
Samenwerken en communiceren medewerkers	Grondslag	Uitvoeren van een overeenkomst (i.c. de arbeidsovereenkomst)
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie	**Beoordeling rechtmatigheid**	
Samenwerken en communiceren extern	Grondslag	• Uitvoeren van een overeenkomst (bijv. inkoop of overeenkomst van opdracht) • Uitvoeren van publieke taak (communicatie met overheidsinstanties) • Gerechtvaardigd belang (overige externe contacten)
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie	**Beoordeling rechtmatigheid**	
Samenwerken en communiceren ouders	Grondslag	Uitvoeren van publieke taak (o.a. artikel 11 WPO, artikel 23b WVO, artikel 20 WEC, Leerplichtwet)
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie	**Beoordeling rechtmatigheid**	
Samenwerken en communiceren leerlingen	Grondslag	Uitvoeren van publieke taak (artikel 8 WPO, artikel 2 WVO, artikel 9 WEC)
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee

		Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie	Beoordeling rechtmatigheid	
Onderwijs-ondersteuning: instroom, doorstroom, uitstroom	Grondslag	Wettelijke verplichting (artikel 40b WPO, artikel 27b WVO, artikel 42a WEC)
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie	Beoordeling rechtmatigheid	
Onderwijs-voorbereiding	Grondslag	Uitvoeren van publieke taak (artikel 8 WPO, artikel 2 WVO, artikel 9 WEC)
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie	Beoordeling rechtmatigheid	
Passend onderwijs	Grondslag	Uitvoeren van publieke taak (artikelen 8 en 18a WPO, artikelen 2 en 17a WVO, artikelen 9 en 28a WEC)
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie	Beoordeling rechtmatigheid	
Ict-ondersteuning	Grondslag	Gerechtvaardigd belang, namelijk veiligheid en continuïteit van de bedrijfsvoering van de onderwijsinstelling
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie	Beoordeling rechtmatigheid	
Informatiebeveiliging en privacy	Grondslag	Gerechtvaardigd belang, namelijk veiligheid en continuïteit van de bedrijfsvoering van de onderwijsinstelling
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee

		Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie	Beoordeling rechtmatigheid	
Realisatie en onderhoud van digitale toegankelijkheid	Grondslag	Gerechtvaardigd belang, namelijk veiligheid en continuïteit van de bedrijfsvoering van de onderwijsinstelling
	Dataminimalisatie	Ja/Nee Toelichting:
	Transparantie	Ja/Nee Betrokkenen zijn op de volgende wijze geïnformeerd:

Hoofdbedrijfsfunctie of proces	Beoordeling rechtmatigheid	
Ander doeleinde, namelijk: **<beschrijving doeleinde verwerking>**	Grondslag	<grondslag>
	Dataminimalisatie	Ja/Nee Toelichting: …
	Transparantie	Ja/Nee Betrokkenen zijn op de volgende wijze geïnformeerd: …

** Als uw onderwijsinstelling Google Workspace for Education voor meerdere ‘andere’ doeleinden gebruikt, dan kopieert u deze tabel en vult u daarin uw andere, eigen doeleinden in.

3. Risicoanalyse

Om een risicoanalyse uit te voeren, neemt u kennis van centraal vastgestelde risico's en maatregelen door Google. Vervolgens maakt u een inventarisatie van de implementatie van centraal vastgestelde mitigerende maatregelen te nemen door onderwijsinstellingen. Indien van toepassing analyseert u uw instelling-specifieke risico's en eventuele mitigerende maatregelen (die niet in de DPIA en DTIA zijn overwogen). U stelt daarna vast of de geconstateerde privacy-risico's door de genomen maatregelen in voldoende mate worden beperkt.

3.1 Landelijke risico's en mitigerende maatregelen

3.1.1 Google Workspace for Education

In de DPIA van 2021 zijn hoge privacy-risico's vastgesteld. Deze zijn na overleg tussen SIVON en SURF met Google beperkt doordat Google technische maatregelen heeft genomen, en omdat onderwijsinstellingen organisatorisch en technische maatregelen nemen.

De risico's en maatregelen zijn beschreven in het rapport "Public version Updated Verification Report Workspace for Education – 17 May 2024". De onderwijsinstelling heeft kennis genomen van de inhoud van dit rapport. In de "Technische handleiding voor Google Workspace for Education v3.0" wordt beschreven of en op welke wijze de geconstateerde risico's beperkt kunnen worden.

Tabel 1: initiële hoge risico's geïdentificeerd in de Update DPIA, overeengekomen maatregelen Google, en verificatieresultaten

Nee.	Risico	Overeengekomen verzachtende maatregel Google	Feitelijke maatstaf
1, 2	**Gebrek aan doelbinding Klant- en servicegegevens**	Google verwerkt Persoonsgegevens van klanten en Diagnostische gegevens (inclusief Accountgegevens) alleen als gegevensverwerker, voor drie doeleinden, wanneer dat nodig is: *1. de Diensten en Technische Ondersteuningsdiensten (TSS) waarop de Klant een abonnement heeft, te leveren, te onderhouden en te verbeteren;* *2. veiligheidsbedreigingen, risico's, bugs en andere anomalieën identificeren, aanpakken en verhelpen* 3. *het ontwikkelen, leveren en installeren van updates voor de Diensten waarop de Klant heeft ingetekend (met inbegrip van nieuwe functionaliteit met betrekking tot de Diensten waarop de Klant heeft ingetekend).*	Risico beperkt door contractuele maatregelen in Privacy Amendement.
		Google verwerkt geen Persoonsgegevens van Klanten en/of Servicegegevens voor advertentiedoeleinden of voor profilering, gegevensanalyse en marktonderzoek.	Risico beperkt door contractuele maatregelen in Privacy Amendement.
		7 geïdentificeerde doeleinden waarvoor Google als onafhankelijke	* **Opmerking**: Google schrijft in het GCPN-addendum dat het de Dienstgegevens kan gebruiken om

		gegevensbeheerder Diagnostische gegevens verder mag verwerken. 1. facturering en accountbeheer en klantrelatiebeheer en gerelateerde correspondentie met Klanten en Klantbeheerders; 2. het verbeteren en optimaliseren van de prestaties en kernfunctionaliteit van toegankelijkheid, privacy, beveiliging en efficiëntie van de IT-infrastructuur van de Clouddiensten en TSS; 3. interne rapportage, financiële rapportage, inkomstenplanning, capaciteitsplanning en prognosemodellering (inclusief productstrategie); 4. opsporen, voorkomen en beschermen van misbruik (zoals automatisch scannen op overeenkomsten met identificatoren van CSAM, scannen op virussen en scannen om overtredingen van de AUP op te sporen); 5. verwerking van Persoonsgegevens in supporttickets en supportverzoeken (inclusief correspondentie met Klanten en Klantbeheerders, en eventuele bijlagen daarbij) die door Beheerders naar Google worden verzonden; 6. Feedback ontvangen en gebruiken; en 7. voldoen aan wettelijke verplichtingen. Voor de duidelijkheid: **het renderen van TSS is een processoractiviteit**. Google zal ervoor zorgen dat **andere doeleinden in de Google Cloud Privacy Notice niet van toepassing zijn op het gebruik van Workspace door Nederlandse scholen en universiteiten.** Met betrekking tot het scannen van inhoud op materiaal voor seksueel misbruik van kinderen (CSAM) en het rapporteren van 'hits' aan het NCMEC, zal Google voldoen aan de toepasselijke wettelijke richtlijnen van het EDPB.	aanbevelingen te doen over gerelateerde producten (d.w.z. producten waarop de Klant geen abonnement heeft), wat niet is toegestaan onder het Privacy Amendement. Laag risico omdat de voorwaarden in het Privacy Amendement prevaleren boven informatie van Google.
		Google verzekert dat machinaal leren om de inhoud van gegevens die zijn verzameld met de spelling- en grammaticacontrole te verbeteren, beperkt is tot het eigen domein van de klant.	Google schrijft in zijn implementatiehandleiding voor gegevensbescherming voor Workspace for Education: "*Het is belangrijk om te benadrukken dat uw Klantgegevens niet worden gebruikt om Spelling & grammatica-services voor accounts van andere klanten te verbeteren*."

		Definitie van anonimisering opgenomen in het Privacyamendement, in overeenstemming met de WP29-richtsnoeren voor anonimiseringstechnieken.	Risico beperkt door contractuele maatregelen in Privacy Amendement.
		In het raamcontract is vastgelegd hoe Google omgaat met *knevelbevelen* wanneer het bevel wordt gegeven om Inhoud en diagnostische gegevens vrij te geven aan rechtshandhavingsinstanties.	In Privacy Amendement en informatie in het openbaar whitepaper.
		Google zet de standaardinstelling voor advertentiepersonalisatie op Uit voor nieuwe eindgebruikers (relevant voor het gebruik van *Aanvullende services*).	Corrigeer de standaardinstelling in Workspace for Education voor nieuwe gebruikers.
3, 4, 7[8]	**Gebrek aan transpa-valuta klant- en servicege gevens**	Google zal een inspectietool ontwikkelen om beheerders toegang te geven tot de telemetriegegevens, inclusief het gebruik van functies	Google heeft een Diagnostic Information Tool (DIT) ontwikkeld die telemetriegebeurtenissen toont (die ook Content Data kunnen bevatten). De toegangsperiode beslaat alleen de laatste 24 uur, vanwege de lange hersteltijd. Daarnaast kunnen Nederlandse beheerders oudere telemetriegegevens opvragen als antwoord op een verzoek om toegang voor een betrokkene.
		Google zal een Helpcentrum-artikel publiceren met gedetailleerde informatie over de categorieën en doeleinden van de verwerking van diagnostische gegevens (waaronder gegevens die zijn verzameld van cloudservers en telemetriegebeurtenissen (atomen) van Android).	Google heeft een nieuwe uitlegpagina gepubliceerd over de DIT en de inhoud van de telemetriegegevens. Deze pagina bevat een algemene beschrijving van de bewaarperioden. "*We bewaren de meeste typen Servicegegevens gedurende een vaste periode van maximaal 180 dagen*. (..) *In de praktijk worden diagnostische gegevens bewaard voor kortere perioden van 30 tot 63 dagen.* Google verwijst ook naar zijn Google Cloud Privacy Notice. Hierin worden de 3 criteria beschreven die Google hanteert om Servicegegevens voor langere perioden te bewaren. Dit zijn: 1. *Beveiliging, preventie van fraude en misbruik,* 2. *Voldoen aan wettelijke of regelgevende vereisten en*

[8] De risico's waren: Gebrek aan transparantie Klantgegevens, Gebrek aan transparantie Diagnostische gegevens, Gebrek aan controle derde partijen / verwerkers.

			3. *Voldoen aan fiscale, boekhoudkundige of financiële vereisten*
		Google heeft bevestigd dat alle subverwerkers die Diagnostische gegevens verwerken, ook Klantgegevens verwerken en daarom al zijn opgenomen in de lijst van subverwerkers voor Klantgegevens. Google zal details over zijn subverwerkers verstrekken, met name voor de Diagnostische gegevens. Google zal het volgende specificeren ○ volledige naam van de entiteit, ○ relevante dienst(en), ○ locatie(s) waar de gegevens worden verwerkt, ○ activiteit (d.w.z. wat doet de subprocessor, ○ of de subverwerker Servicegegevens verwerkt in tijdelijke, persoonlijke en/of archieflogboeken.	Google heeft de informatie over zijn subverwerkers en filialen uitgebreid, welke persoonlijke gegevens zij voor welke doeleinden kunnen inzien. De lijst van subverwerkers bevat bedrijven en gelieerde bedrijven in twee lijsten van derde landen. Google heeft de afgesproken extra informatie over de subverwerkers aan SURF en SIVON verstrekt en heeft samengewerkt met de DTIA om de risico's van doorgifte naar derde landen in te schatten. Het DTIA concludeert dat er geen hoge doorgifterisico's zijn voor persoonsgegevens via Meet, mits scholen (i) een betaalde versie van Workspace gebruiken en (ii) kiezen voor opslag in de EU van Content Data. Als ze speciale gegevenscategorieën willen uitwisselen via Meet, moeten ze (iii) Client-Side Encryption toepassen om het risico van ongeautoriseerde toegang tot deze gegevens in derde landen uit te sluiten.
		Google toont een profielfoto van een eindgebruiker op de landingspagina voor alle Workspace Core Services (zowel web als mobiel). Deze foto verdwijnt wanneer de eindgebruiker de privacybeschermde Workspace-services verlaat. Google verplicht zich om reguliere Workspace-accounts automatisch uit te loggen wanneer ze uitgeschakelde *Aanvullende services* bezoeken en een waarschuwing weer te geven aan K-12-gebruikers.	Google heeft de overeengekomen maatregelen toegepast. Wanneer *Aanvullende services* zijn uitgeschakeld in een K-12-omgeving, geeft Google een waarschuwing weer aan eindgebruikers wanneer ze toegang willen krijgen tot deze uitgeschakelde services.
		Google zal alle relevante juridische informatie over het Google Workspace-account permanent beschikbaar stellen in een kennisgeving voor eindgebruikers.	De pop-up is verbeterd en gepersonaliseerd. De relevante juridische informatie is niet permanent beschikbaar via het inlog- of Google-accountmenu. Google heeft toegezegd bepaalde UI-wijzigingen door te voeren voor [**datum vertrouwelijk**].

		Google zal een Domain Wide Takeout-mogelijkheid ontwikkelen op het niveau van individuele gebruikers/orga-eenheden.	Google heeft informatie over de organisatorische Data Export gepubliceerd op https://support.google.com/a/answer/12940323 en https://support.google.com/a/answer/100458 Gegevens moeten worden geëxporteerd naar het Google Cloud Platform. Google heeft ervoor gezorgd dat de beheerder de (verwerkers)voorwaarden uit het Cloud Data Processing Addendum moet accepteren. Voor deze use case is GCP geen Workspace *Additional Service*.
		Google geeft een nieuwe waarschuwing aan eindgebruikers in het feedbackformulier om geen gevoelige gegevens met Google te delen	Google toont een pop-up met een waarschuwing.
		Google zal de uitleg aan beheerders in de Implementatiehandleiding Gegevensbescherming verbeteren dat Google Accountgegevens verwerkt als verwerker wanneer het Google-account wordt gebruikt in de Core Services.	Google biedt een verklaring.
		Google zal de beschikbaarheid van admin-auditlogs uitbreiden naar alle Core Services.	Google levert veel meer auditlogs, in overeenstemming met het saneringsplan - voor zover getest.
5, 6	**Geen wettelijke grond voor Google en scholen/universiteiten + Ontbrekende privacycontroles**	Met betrekking tot de (afzonderlijke) wettelijke grond voor het uitlezen van cookie- en telemetriegegevens van eindgebruikersapparaten, zoals gedefinieerd in de ePrivacy-richtlijn, zal Google de richtlijnen van de regelgeving volgen.	Google legt de noodzaak van het opnemen van Inhoudsgegevens in telemetriegebeurtenissen over Spelling- en grammaticatelemetriegebeurtenissen uit in een apart onderwerp op de nieuwe DIT-informatiepagina, onder *Spelling- en grammaticasuggesties*. Het is aannemelijk dat deze gegevensverzameling is vrijgesteld van toestemming onder de Nederlandse analytische toestemmingsuitzondering.
		Google stemt er contractueel mee in dat toestemming van de eindgebruiker niet van toepassing is als grond voor het delen van Servicegegevens met derden wanneer de services van die partijen door de Klant zijn uitgeschakeld (inclusief Google als derde partij voor *Aanvullende Services*).	Opgenomen in het Privacy-amendement.
		Google logt Workspace-eindgebruikers automatisch uit wanneer ze toegang hebben tot (**ingeschakelde**) *Aanvullende services*.	Admins kunnen de toegang tot alle *Extra diensten* uitschakelen.

		Google wordt een gegevensverwerker voor de diagnostische gegevens en voor het bieden van ondersteuning, maar niet voor de feedbackgegevens. Scholen wordt geadviseerd hun medewerkers te waarschuwen geen gebruik te maken van Feedback.	Google is gegevensverwerker voor de levering van TSS volgens Privacywijziging, maar mag ook Support Data *verder* verwerken als gegevensbeheerder. Zowel de verwerking van Feedbackgegevens als de verdere verwerking van Supportgegevens zijn overeengekomen legitieme zakelijke doeleinden.
		Admins kunnen het gebruik van *Additional Services* verbieden als ze zijn aangemeld met een Workspace Enterprise-account.	Admins kunnen de toegang tot alle *Extra diensten* uitschakelen.
8	**Geen toegang voor betrokkenen**	Google gaat individuele TakeOut-tool ontwikkelen	Google biedt 3 verschillende tools voor beheerders en eindgebruikers om persoonlijke gegevens te exporteren (Data Export, Google Vault en Google Takeout). Deze tools zijn gericht op Inhoudsgegevens, met enkele activiteitenlogboeken (*gegevens die eigendom zijn van gebruikers*). Deze zelfbedieningshulpmiddelen bieden geen toegang tot alle Servicegegevens, maar beheerders kunnen diagnostische en telemetriegegevens exporteren en eindgebruikers kunnen het DSAR-formulier van Google gebruiken om toegang te vragen tot persoonlijke gegevens die Google verwerkt als gegevensbeheerder.
		Google biedt geen geïndividualiseerde toegang tot diagnostische gegevens, telemetriegegevens en logbestanden over webservertoegang/cookiegegevens (Google noemt deze gegevens servicedata). Beheerders kunnen sommige diagnostische gegevens verzamelen door de uitgebreide auditlogs te exporteren en individuele gebruikersgegevens op te vragen. De DIT geeft alleen toegang tot de laatste 24 uur.	Admins moeten BigQuery gebruiken om auditlogs te exporteren. Google heeft ervoor gezorgd dat de beheerder de (verwerkers)voorwaarden van het Google Cloud Processing Addendum moet accepteren. Voor deze use case is GCP geen Workspace *Additional Service.* Google stelt superbeheerders ook in staat om toegang te vragen tot historische telemetriegegevens.
		Google zal details publiceren waarom het over het algemeen geen toegang kan verlenen tot telemetriegegevens, websitegegevens en persoonsgegevens uit de SIEM-beveiligingslogboeken van Google. Google heeft bevestigd dat het elk verzoek zal beoordelen onder Artikel 15 GDPR (d.w.z. geen standaard afwijzing).	Nieuwe uitleg gepubliceerd onder *Informatie die niet is verstrekt als antwoord op een verzoek om toegang*.

		Het ontwerp van het DSAR-formulier van Google is niet gebruiksvriendelijk: gebruikers weten niet welke categorieën gegevens Google verwerkt.	Scholen en universiteiten kunnen de uitleg in dit rapport gebruiken om werknemers en studenten te helpen toegang te vragen tot al hun persoonlijke gegevens, via zelfbedieningstools, via hun admin en via het DSAR-formulier van Google.
9	**Doorgifte van persoonlijke gegevens naar de VS + gebrek aan controle over subverwerkers**		De risico's van doorgifte van de zes categorieën persoonsgegevens worden beoordeeld in de afzonderlijke DTIA. Het DTIA concludeert dat er geen grote risico's zijn voor de overdracht van persoonsgegevens via Meet, als (i) scholen een betaalde versie van Workspace gebruiken en (ii) kiezen voor opslag van inhoudsgegevens in de EU. Als ze speciale gegevenscategorieën willen uitwisselen via Meet, moeten ze (iii) Client-Side Encryption toepassen om het risico van ongeautoriseerde toegang tot deze gegevens in 7 derde landen uit te sluiten.

3.1.2 Data Transfer Impact Assessment

In de DPIA die in 2021 is uitgevoerd, is vastgesteld dat er persoonsgegevens worden uitgewisseld met de Verenigde Staten. Hiervoor is een zogenaamde Data Transfer Impact Assessment (DTIA) uitgevoerd. Hierbij worden privacyrisico's onderzocht van doorgifte van gegevens naar landen buiten de Europese Economische Ruimte (EER). De DTIA – inclusief de implementatie van eventuele maatregelen die hieruit voortvloeien – is in 2024 afgerond. De DTIA is opgenomen in het rapport "Public version DTIA Google Meet (Workspace for Education) – 11 April 2024". In de "Technische handleiding voor Google Workspace for Education v3.0" wordt beschreven of en op welke wijze de in de DTIA geconstateerde risico's beperkt kunnen worden.

Public version DTIA Google Meet (Workspace for Education) – 11 April 2024:

Inhoudelijke gegevens (content data)

Met het oog op het bovenstaande en de toepasselijke wetgeving inzake gegevensbescherming is de overdracht van gevoelige en speciale gegevenscategorieën (bijzondere persoonsgegevens) zonder client side encryption:	niet toegestaan
Met het oog op het bovenstaande en de toepasselijke wetgeving inzake gegevensbescherming is de overdracht van reguliere persoonsgegevens:	toegestaan

Accountgegevens (account data)

Met het oog op het bovenstaande en de toepasselijke wetgeving inzake gegevensbescherming is de overdracht:	toegestaan

Ondersteunende gegevens (support data)

Met het oog op het bovenstaande en de toepasselijke wetgeving inzake gegevensbescherming is de overdracht:	toegestaan

Diagnostische gegevens (diagnostic data)

Met het oog op het bovenstaande en de toepasselijke wetgeving inzake gegevensbescherming is de overdracht:	toegestaan

Beveiligingsgegevens, T&S (security data, T&S)

Met het oog op het bovenstaande en de toepasselijke wetgeving inzake gegevensbescherming is de overdracht:	toegestaan

Websitegegevens (website data)

Met het oog op het bovenstaande en de toepasselijke wetgeving inzake gegevensbescherming is de overdracht:	toegestaan

3.1.3 Nieuwe bevindingen Google Workspace for Education

Tijdens de uitvoering van de DPIA en het controleren van de maatregelen die Google heeft genomen, kwamen er in 2023 vijf nieuwe privacy-risico's in beeld. Ook hierover hebben SIVON en SURF met Google overleg gevoerd met Google om deze nieuwe risico's te beperken. In het rapport "Public version New findings review Google Workspace for Education – 16 May 2024" zijn de risico's en de genomen maatregelen beschreven. In de "Technische handleiding voor Google Workspace for Education v3.0" wordt beschreven of en op welke wijze de geconstateerde risico's beperkt kunnen worden.

Tabel 1: (potentieel) hoge risico's, bevindingen, maatregelen van Google en aanbevolen maatregelen voor scholen/universiteiten

Oorspronkelijke risico('s)	vinden	Maatregel genomen door Google	Aanbevolen maatregel voor scholen en universiteiten
Gebrek aan doelbinding Klantgegevens en diagnostische gegevens	Google kan enquêtes tonen aan eindgebruikers in de Core Services.	Google heeft bevestigd dat het geen enquêtes zal tonen aan K-12 gebruikers.	Scholen en universiteiten moeten de K-12 instelling kiezen in hun tenant, zelfs als hun gebruikers 18+ zijn. Google heeft bevestigd dat het de werkelijke leeftijd van Education-huurders niet zal controleren.
Gebrek aan doelbinding Klantgegevens Geen wettelijke grond voor Google	Introductie van *slimme functies* zoals Smart Compose die machine learning	*Slimme functies* zijn standaard uitgeschakeld voor domeinen in Europa, maar	

en scholen/universiteit en Standaard geen privacy	gebruiken. Rol van Google niet duidelijk/niet gedocumenteerd. Gebruikers worden aangespoord om de services in te schakelen.	gebruikers kunnen deze nog steeds inschakelen. Google heeft toegezegd alle Inhoud en diagnostische gegevens van Smart Features te verwerken binnen de rol van verwerker (afgezien van de beperkte overeengekomen legitieme zakelijke doeleinden) en de resultaten blijven binnen het domein van de klant.	
Geen wettelijke grond voor Google en scholen/universiteit en Ontbrekende privacycontroles	Gebruik van het multifunctionele NID-cookie bij het inloggen op een Workspace-account en bij het opzoeken van de Google Cloud Privacy Notice.	Google heeft SURF en SIVON geïnformeerd dat het de NID-cookie die is ingesteld in de Workspace-omgeving of bij het opzoeken van de Google Cloud Privacy Notice niet gebruikt voor advertentiedoeleinden. Bij het afmelden moeten gebruikers toestemming geven voor het gebruik van het NID-cookie en andere niet-essentiële cookies voor advertenties op Google-websites en op websites van derden met Google-reclame.	-
		Google heeft de tekst van de cookiebanner op de GCPN-pagina verbeterd om aan te kondigen dat de GCPN-site geen cookies gebruikt voor advertenties.	
Gebrek aan transparantie	Google verzamelt Inhoudsgegevens van spellingcontrole in telemetriegebeurtenissen en direct	Google heeft uitgelegd en op 9 juni 2023 een verklaring gepubliceerd waarom het nodig is om deze gegevens te verzamelen en	-

	identificeerbare persoonsgegevens (naam/e-mailadres). De bewaarperiode van deze gebeurtenissen is onbekend.	uitgelegd dat de bewaartermijn 30 dagen is.	
Geen wettelijke grond voor Google en scholen/universiteiten	Nieuwe richtlijnen van de EDPB over hoge risico's van CSAM-scanning.	Google heeft bevestigd dat het alleen scant op **bekende** CSAM, er wordt geen gebruik gemaakt van machine learning/AI.	-

3.1.4 ChromeOS en Chromebrowser op beheerde chromebooks

Uit de DPIA van 2021 kwam naar voren dat er aan het gebruik van ChromeOS en Chromebrowser op chromebooks (gebruikt door leerlingen en/of medewerkers) ook privacy-risico's kleven. SIVON en SURF zijn een onderzoek gestart naar deze hoge privacy-risico's. Deze risico's zijn na overleg tussen SIVON en SURF met Google beperkt doordat Google technische maatregelen heeft genomen, en een specifieke 'Data processor mode' (verwerkersversie) van ChromeOS voor Nederlanse onderwijsinstellingen beschikbaar heeft gesteld. De uitkomsten van het onderzoek zijn opgenomen in het rapport "Public version Verification Report Processor version Google Chrome for Education – 7 March 2024". In de "Handleiding ChromeOS en Chrome-browser 2024" wordt beschreven of en op welke wijze de geconstateerde risico's beperkt kunnen worden.

Tabel 1: Gecombineerde resultaten van de eerste inspectie en dit verificatierapport

Uitgave	Aanbevolen mitigerende maatregelen scholen	Mitigerende maatregelen genomen door Google
DSAR-resultaten onvolledig (inzageverzoek betrokkenen)	Blijf de toegang tot de Chrome Web Store en de Google Play Store blokkeren.	Toezegging om een individuele beoordeling van elke DSAR te doen
	Gebruik de richtlijnen van SIVON om leerlingen te informeren hoe ze toegang kunnen aanvragen bij de school en bij Google.	Google is een verwerker voor de Domain-wide Takeout tool voor beheerders
		Google is een verwerker voor de individuele Takeout-tool voor eindgebruikers
		Google heeft documentatie gepubliceerd over welke diagnostische/telemetriegegevens de essentiële Chroomservices verzamelen, in veel verschillende Help-artikelen per Chroomservice, voor zover ze überhaupt gebruikers- of apparaatgerelateerde gegevens verzamelen. De helpartikelen zijn toegankelijk via hyperlinks in de lijst met essentiële en optionele Chroomservices.

		Google heeft meer informatie gepubliceerd over het bewaren van Chrome-gegevens in een helpartikel over het bewaren van Workspace-gegevens.
		Google heeft een Service Data Downloader ontwikkeld voor beheerders
DSAR weigering onvoldoende uitgelegd	Gebruik de beschikbare logboeken met admingebeurtenissen om toegang te krijgen tot persoonlijke gegevens.	Het beheerde ChromeOS bevat services om toegang te krijgen tot de gegevens, zoals de Service Data Downloader en Diagnostic Information Tool (DIT, een telemetriegegevensviewer die is ontwikkeld voor Workspace).
		Google heeft een verbeterde uitleg gepubliceerd waarom het de toegang tot sommige persoonlijke gegevens kan weigeren.
		Google heeft documentatie gepubliceerd over welke categorieën persoonlijke gegevens, met betrekking tot welke service, beschikbaar zijn in de gebeurtenislogboeken voor beheerders.
Gebrek aan doelbinding gegevens Takeout tool	Blijf de Workspace *Additional* Services uitschakelen.	Google is een gegevensverwerker geworden voor de Takeout-tools voor beheerders en eindgebruikers.
Gebrek aan doelbeperking ChromeOS en browser	Meld u aan voor de nieuwe ChromeOS- en browserprocessorovereenkomst.	De verwerkersovereenkomst voor het beheerde ChromeOS en de browser bevat twee limitatieve lijsten met doeleinden, voor Google als verwerker en voor overeengekomen verdere verwerking door Google als verwerkingsverantwoordelijke voor zijn legitieme zakelijke doeleinden.
	Schakel de *optionele Chrome Services* niet in, waarvoor Google blijft fungeren als controller (al uitgeschakeld voor nieuwe klanten).	
	Selecteer de instelling K-12 (ook universiteiten) om verwerking voor commerciële doeleinden te blokkeren, zoals groepsprofilering in Privacy Sandbox en de standaardpresentatie van enquêtes.	
Gebrek aan doelbeperking Synchroniseer gegevens buiten Workspace for Education	Hoewel het gebrek aan doelbeperking is opgelost, wordt scholen nog steeds geadviseerd om Chrome Sync niet in te schakelen als de gebruikers de Google-accounts voor privédoeleinden mogen	Op basis van de verwerkersovereenkomst voor het beheerde ChromeOS en de browser is Google een gegevensverwerker voor Chrome Sync, zowel voor de Inhoud als voor de Diagnostische gegevens (los van Workspace for Education, waar Sync al een verwerkersdienst is).

	gebruiken - vanwege de overdrachtsrisico's.	
Gebrek aan doelbeperking (Beheerd) Play Store en Chrome Webstore	Schakel de toegang tot alle *Aanvullende* services in Workspace uit, inclusief de (beheerde) Play Store en de Chrome Webstore. Als scholen leerlingen in staat willen stellen om geselecteerde toegestane apps te gebruiken, moeten ze deze apps via hun eigen netwerk distribueren. Voor browserextensies kunnen ze Force install toepassen, zonder dat gebruikers de Chrome webstore hoeven te bezoeken.	Google heeft geen maatregelen aangekondigd.
Geen geldige reden voor overdracht van persoonlijke gegevens naar de VS	Meld u aan voor de nieuwe verwerkersovereenkomst en pas alle maatregelen voor gegevensminimalisatie uit de bijgewerkte richtlijnen van SIVON toe, inclusief alle stappen in de handleiding.	Google is een gegevensverwerker geworden voor het beheerde ChromeOS en de browser. De Nederlandse onderwijsklanten vertrouwen op passende overdrachtsmechanismen onder hoofdstuk V GDPR.
	Schakel SafeSites uit met een registerinstelling (overweeg het gebruik van een filter van derden).	Google heeft niet gereageerd op het verzoek om lokale filtering toe te staan in plaats van URL's met de IP-adressen door te sturen naar de VS.
	Scholen moeten alle privacyvriendelijke instellingen centraal afdwingen, inclusief het uitschakelen van de toegang tot google.com en youtube.com, ofwel door het gebruik van een proxyserver af te dwingen om de functionaliteit op het lokale netwerk te blokkeren, of via handmatige URL-blokkeeropties in de beheerconsole.	Google biedt centrale beheeropties voor de gastmodus op beheerde Chromebooks, waaronder het blokkeren van cookies van derden.
	Scholen wordt (nog steeds) afgeraden om Chrome Sync in te schakelen als de gebruikers de Google-accounts mogen gebruiken voor privédoeleinden, waaronder privé e-mails en privé surfgedrag waaruit speciale gegevenscategorieën kunnen worden afgeleid - vanwege het risico op ongeautoriseerde toegang door overheidsinstanties in 7 derde landen.	Google geeft de persoonsgegevens door aan 7 derde landen. De Nederlandse onderwijsklanten vertrouwen op passende overdrachtsmechanismen onder hoofdstuk V GDPR Uit de DTIA die is uitgevoerd voor Google Workspace Meet volgt dat overdracht van bijzondere categorieën gegevens leidt tot een hoog risico als scholen deze gegevens niet kunnen versleutelen met een lokaal bewaarde sleutel.

	Schakel Sync uit door het beleid *SyncDisabled* op *true* te zetten of zorg ervoor dat leerlingen een zelfbeheerde lokale wachtwoordzin gebruiken om de Sync-gegevens te versleutelen.	Google heeft nog geen beleid ontwikkeld voor beheerders om het gebruik van versleuteling van de Chrome Sync-gegevens met lokaal bewaarde sleutels centraal af te dwingen op de apparaten van eindgebruikers.
Privacy-onvriendelijke standaardinstellingen	Handhaaf waar mogelijk de aanbevolen privacy-vriendelijke instellingen.	Privacy Sandbox-proeven zijn uitgeschakeld voor gebruikers jonger dan 18 jaar.
		Google heeft niet gereageerd op het verzoek om de trackingbeschermingsfuncties in de Chrome-browser te verbeteren wanneer cookies van derden zijn geblokkeerd, het DNT-signaal is ingeschakeld en het vooraf laden van websites is uitgeschakeld. Bijvoorbeeld door verkeer naar Google-services te blokkeren waarbij Google niet optreedt als gegevensverwerker (zoals analytics en fonts). Google legt uit dat beheerders beleidsregels kunnen gebruiken om cookies en javascript van derden, waaronder Google, te beperken.
	De Privacy Sandbox uitschakelen voor alle gebruikers (is al uitgeschakeld als scholen het advies opvolgen om de K-12 instelling te kiezen	Google heeft beheerders controle gegeven over het blokkeren van advertentiepersonalisatie en metingen als onderdeel van Privacy Sandbox in de processorversie van het beheerde ChromeOS.
Gebrek aan transparantie	Schakel de toegang tot de (beheerde) Play Store en Chrome Webstore uit.	Google heeft geen maatregelen aangekondigd.

3.1.5 Transparantie door onderwijsinstelling

Een belangrijk onderdeel in de DPIA is transparantie: betrokkenen (leerlingen, hun ouders en medewerkers) moeten weten hoe en welke persoonsgegevens worden gebruikt door Google. Google geeft betrokkenen daar meer informatie over. Voor Workspace for Education gebruikers in het Nederlandse onderwijs is een aparte pagina beschikbaar[9]. Het is belangrijk voor de onderwijsinstelling om ook zelf betrokkenen te informeren over de uitkomsten van de DPIA. SIVON heeft voorbeeldbrieven gemaakt voor leerlingen (en hun ouders als de leerling jonger is dan 16 jaar)[10], medewerkers[11] en de GRM en Raad van Toezicht[12].

[9] https://services.google.com/fh/files/misc/gcpnaddendum_jan_23_nl.pdf
[10] https://sivon.nl/voorbeeldbrief-google-workspace-ouders-verzorgers/
[11] https://sivon.nl/voorbeeldbrief-google-workspace-leerkrachten-en-docenten/
[12] https://sivon.nl/voorbeeldbrief-mr-en-rvt/

SIVON heeft voor beheerders (administrators), privacy officers en functionarissen voor gegevensbescherming een aanvullende uitleg[13] gemaakt over transparantie en gegevensverwerkingen binnen Google Workspace for Education. Deze informatie geeft onder andere inzicht in de verschillende beschikbaar tooling om inzage te krijgen en geven in de verschillende persoonsgegevens die Google verwerkt.

3.1.6 Aanbevelingen Google beveiligingsmaatregelen

Bij het veilig en verantwoord omgaan met persoonsgegevens, horen ook de juiste beveiligingsinstellingen. SIVON heeft in samenwerking met Google een aantal *aanbevelingen* voor beveiligingsinstellingen[14] opgesteld voor Google Workspace for Education. Overweeg om deze aanbevolen instellingen te gebruiken.

3.2 Lokale DPIA

3.2.1 Vaststelling centraal vastgestelde risico's en mitigerende maatregelen

[NAAM ONDERWIJSINSTELLING] heeft de hiervoor opgesomde centraal vastgestelde risico's en mitigerende maatregelen overwogen en stelt deze vast al de risico-afweging voor de eigen organisatie. Het oordeel is dat de risico's [voldoende/onvoldoende] worden beperkt voor het (voortgezet) gebruik van Google Workspace for Education en/of ChromeOS en Chromebrowser op beheerde chromebooks.

Zijn de door Google en onderwijsinstelling getroffen en nog te treffen maatregelen voldoende om de hoge risico's voor uw onderwijsinstelling weg te nemen?	**Ja/Nee**
Deze beoordeling is gebaseerd op de volgende documenten:	
1. Public version Updated Verification Report Workspace for Education – 17 May 2024	
2. Public version DTIA Google Meet (Workspace for Education – 11 April 2024	
3. Public version New findings review Google Workspace for Education – 16 May 2024	
4. Public version Verification Report Processor version Google Chrome for Education – 7 March 2024	
5. Technische handleiding voor Google Workspace for Education v3.0	
6. Handleiding ChromeOS en Chrome-browser 2024.	

** Deze documenten zijn te vinden op de websites van SIVON en SURF.*

Indien het antwoord op bovenstaande vraag 'Nee' is, dan overweegt [NAAM ONDERWIJSINSTELLING] het volgende over de privacy-risico's en aanvullende mitigerende maatregelen: [overweging].

[13] https://sivon.nl/uitleg-transparantie-gegevensverwerkingen-google-workspace-for-education/
[14] https://sivon.nl/wp-content/uploads/2022/06/Beveiliging-Google-Workspace.pdf

3.2.2 Uitvoering centraal vastgestelde maatregelen

Onderwijsinstellingen moeten allereerst de *Workspace for Education (Online) agreement (aanpassingen overeenkomst (verzonden 9 augustus 2021)* accepteren die door SURF en SIVON zijn onderhandeld. Daarnaast zijn in de *Handleiding technische maatregelen (augustus 2021)* de maatregelen beschreven die een onderwijsinstelling zelf moet nemen om de vastgestelde hoge risico's weg te nemen. Als [NAAM ONDERWIJSINSTELLING]de aangepaste overeenkomst (nog) niet geaccepteerd heeft en (nog) niet al deze maatregelen heeft doorgevoerd, blijven er hoge restrisico's bestaan bij het gebruik van Google Workspace for Education.

In de Technische handleiding voor Google Workspace for Education v3.0 en Handleiding ChromeOS en Chrome-browser 2024 zijn instellingen opgenomen die onderwijsinstellingen zelf moeten doorvoeren om de privacyrisico's te mitigeren. In "BIJLAGE 1: Maatregelen Google Workspace for Education" en "BIJLAGE 2: Maatregelen ChromeOS en Chromebrowser op beheerde chromebooks" is een overzicht opgenomen van de te nemen maatregelen.

Geef hieronder aan welke maatregelen uw onderwijsinstelling (nog) niet heeft doorgevoerd, wat de planning is voor het alsnog nemen van de maatregel of te motiveren waarom is besloten door uw onderwijsinstelling om de maatregel niet door te voeren. Tot slot beschrijf u welke restrisico's het (nog) niet doorvoeren van de maatregel oplevert.

Zijn de maatregelen zoals beschreven in de *Technische handleiding voor Google Workspace for Education v3.0,* die op uw onderwijsinstelling van toepassing zijn, doorgevoerd?				**Ja/Nee***
Zijn de maatregelen zoals beschreven in de *Handleiding ChromeOS en Chrome-browser,* die op uw onderwijsinstelling van toepassing zijn, doorgevoerd?				Ja/Nee*
Indien het antwoord 'Nee' is vul dan onderstaande tabel verder in.				
Beschrijving niet of nog niet uitgevoerde maatregel:	Wordt de maatregel nog uitgevoerd?	Binnen welke termijn is de maatregel uitgevoerd?	Er is besloten de maatregel niet uit te voeren, omdat:	Beschrijving restrisico met risicoclassificatie (laag, midden, hoog)
…	Ja/Nee*	Voor <datum>	…	…
…	Ja/Nee*	Voor <datum>	…	…

* Haal door wat niet van toepassing is.

3.2.4 Organisatie-specifieke risico-afweging en maatregelen

De volgende stap is om vast te stellen of het gebruik van Workspace for Education door uw onderwijsinstelling nog andere privacyrisico's met zich meebrengt. Dit zijn risico's die niet in de centrale DPIA en DTIA zijn of kunnen worden vastgesteld, maar alleen door de onderwijsinstelling zelf. De reden is dat iedere onderwijsinstelling Google Workspace for Education op een andere manier gebruikt. De ene

onderwijsinstelling gebruikt het wellicht alleen voor het delen van digitaal lesmateriaal of het geven van online onderwijs, terwijl een andere onderwijsinstelling het ook gebruikt voor het bijhouden van administratie.

Zijn er daarom gelet op de doeleinden waarvoor binnen uw onderwijsinstelling gebruik gemaakt wordt van Google Workspace for Education, de persoonsgegevens die daarin verwerkt worden en de wijze waarop die verwerkingen technisch en organisatorisch ingebed zijn nog andere risico's dan de bij paragraaf 3.1 beschreven risico's en maatregelen? Om dit te bepalen kunt u bijvoorbeeld gebruik maken van de MAPGOOD-methodiek. Bij ieder element in de MAPGOOD spelen bepaalde risico's, bijvoorbeeld:

- Mens
  - onkunde, slordigheid
  - niet werken volgens voorschriften
  - fraude, sabotage
- Apparatuur
  - verouderd, onjuist functioneren
  - stroomuitval
- Programmatuur
  - ontwerp/programmeerfouten
  - geen actuele updates
- Gegevens
  - ontoegankelijk
  - toegankelijk voor onbevoegden
  - verloren gaan
- Organisatie
  - onduidelijke taken, bevoegdheden
  - ontbrekende gedragscodes
- Omgeving
  - onvoldoende beveiligde ruimtes
  - natuurgeweld
- Diensten
  - geen goede leveranciersafspraken
  - leverancier gaat failliet

Door privacyrisico's in deze categorieën in te delen wordt meteen voorgesorteerd op de mogelijke maatregelen. Zo vraagt een dreiging in de categorie 'Mens' vaak om maatregelen op het gebied van awareness of training.

Na het vaststellen van de risico's beoordeelt u of de risico's beperkt kunnen worden door bestaande of nieuwe maatregelen te nemen. Dit wordt het mitigeren van risico's genoemd. Het risico, na toepassing van de mitigerende maatregelen, wordt restrisico genoemd.

Vervolgens is het van belang om vast te stellen hoe groot de gevonden risico's zijn. Dit heet de classificatie van een risico. Daarbij wordt de kans dat een dreiging optreedt vermenigvuldigd met de impact, ofwel de

schade die wordt aangericht. Wij gaan uit van een schaalverdeling van 3; op die manier kan de classificatie van het risico waardes aannemen tussen 1 en 9.

Het risico – voor de betrokkene – wordt beoordeeld aan de hand van de volgende indeling en berekening:

kans (waarschijnlijkheid) X impact (ernst) -/- de risico-mitigerende maatregelen = restrisico

Risico	Kans Laag (1)	Kans Midden (2)	Kans Hoog (3)
Impact Hoog (3)	Risico Midden (Score: 3)	Risico Hoog (Score: 6)	Risico (zeer) hoog (Score: 9)
Impact Midden (2)	Risico Laag (Score: 2)	Risico Midden (Score: 4)	Risico Hoog (Score: 6)
Impact Laag (1)	Risico Zeer laag (Score: 1)	Risico Laag (Score: 2)	Risico Midden (Score: 3)

Een restrisico-score van 1 en 2 is een laag risico, een score van 3 of 4 is gemiddeld, een score van 6 of 9 is hoog. Bij het vaststellen van een gemiddeld risico, moet overwogen worden of het risico zich op – korte of langere termijn – kan realiseren tot een hoog privacy-risico.

In onderstaande tabel beschrijft u organisatie-specifieke risico's die u binnen uw onderwijsinstelling heeft vastgesteld, inclusief de mitigerende maatregelen en de classificatie van het restrisico. Het gaat hierbij dus om risico's en maatregelen die niet centraal zijn vastgesteld en geadviseerd.

Als u in paragraaf 2.4 bij de beoordeling van de rechtmatigheid van de verwerkingen heeft vastgesteld dat niet (volledig) is voldaan aan de eisen van dataminimalisatie en transparantie, dan neemt u die risico's en maatregelen ook over in onderstaande tabel.

Beschrijving organisatie-specifiek risico	Mitigerende maatregel(en)	Binnen welke termijn is de maatregel uitgevoerd?	Classificatie risico (laag, midden, hoog) na uitvoering maatregel (restrisico)
…	…	…	…
…	…	…	…
…	…	…	…

4. Conclusie en vaststelling

4.1 Vaststelling risico-afweging en maatregelen

Op basis van het onderzoek dat in het kader van de centrale DPIA, DTIA Google Workspace for Education en ChromeOS en Chrome-browser op beheerder chromebooks is uitgevoerd, is de conclusie van [NAAM ONDERWIJSINSTELLING] dat de gevolgen voor de rechten en vrijheden van deze betrokkenen door de verwerking van persoonsgegevens van leerlingen en medewerkers - na toepassing van risico-mitigerende maatregelen – in [onvoldoende/voldoende] mate zijn beheerst. De in hoofdstuk 3 genoemde (rest)risico's worden geaccepteerd. Deze conclusie wordt anders als de hierna genoemde risico-mitigerende maatregelen door of namens het bestuur (bevoegd gezag) niet of onvoldoende worden uitgevoerd.

De genomen en te nemen maatregelen, waarborgen, veiligheidsmaatregelen en mechanismen die binnen [Google Workspace for Education en ChromeOS **en/of** Chrome-browser op beheerder chromebooks] de bescherming van persoonsgegevens garanderen, zijn [onvoldoende/voldoende] gericht op het beperken van de risico's voor de rechten en vrijheden van betrokkenen.

Er is [wel/niet] gebleken van hoge risico's voor de rechten en vrijheden van betrokkenen die moet leiden tot een 'voorafgaande raadpleging' bij de Autoriteit Persoonsgegevens zoals omschreven in artikel 36 AVG.

4.2 Risico-mitigerende maatregelen onderwijsinstelling

Bij deze hiervoor genoemde beoordeling zijn een aantal maatregelen geïdentificeerd die moeten worden genomen om de in de (centrale en lokale) DPIA en DTIA vastgestelde privacy-risico's te mitigeren. Het betreffen de hierna te noemen maatregelen waarbij de verantwoordelijkheid voor de implementatie bij het bestuur (bevoegd gezag) als verwerkingsverantwoordelijke ligt.

[NAAM ONDERWIJSINSTELLING] heeft de volgende maatregelen genomen, of heeft deze gepland te nemen:

1. volg de aanbevelingen op uit de Technische handleiding voor Google Workspace for Education v3.0 (zie bijlage 1).
2. [ChromeOS en Chrome-browser op beheerde chromebooks: volg de aanbevelingen op uit de Handleiding ChromeOS en Chrome-browser 2024, zie bijlage 2.]
3. goede gebruiksinstructies voor beheerders en gebruikers (op school), om verkeerd gebruik, misbruik of beveiligingsincidenten te voorkomen. Maak voor beheerders gebruik van de aanvullende uitleg[15] van SIVON over transparantie en gegevensverwerkingen binnen Google Workspace for Education.
4. Zorg voor een betaalde licentie op Google Workspace for Education vanwege de vereiste extra functionaliteit voor gegevensopslag binnen de EU (DTIA) en extra beveiligingsopties.
5. het inregelen van de correcte autorisaties in Google Workspace for Education. Zorg hierbij voor functiescheiding waarbij in geval van autorisatieverlening gewerkt wordt met het vier-ogenprincipe bij beheerdersfunctionaliteiten. Bij accounts van leerlingen moet gekozen worden voor de K-12 functie waarbij de accounts worden aangemerkt als (K-12) leerling.
6. het informeren de betrokkenen over de uitkomsten van de DPIA en de (mogelijke) gevolgen voor hun rechten en vrijheden. Maak hiervoor gebruik van de voorbeeld-brieven van SIVON voor leerlingen en ouders[16], medewerkers[17] en de toezichthouders (GMR/RvT)[18].
7. overweeg om de door Google Workspace aanbevolen beveiligingsinstellingen over zoals beschreven in deze handleiding[19] te nemen.

[15] https://sivon.nl/uitleg-transparantie-gegevensverwerkingen-google-workspace-for-education/
[16] https://sivon.nl/voorbeeldbrief-google-workspace-ouders-verzorgers/
[17] https://sivon.nl/voorbeeldbrief-google-workspace-leerkrachten-en-docenten/
[18] https://sivon.nl/voorbeeldbrief-mr-en-rvt/
[19] https://sivon.nl/wp-content/uploads/2022/06/Beveiliging-Google-Workspace.pdf

8. [Indien van toepassing: Neem de technische en organisatie maatregelen die volgen uit de eigen lokale risico-afweging: [beschrijving maatregelen].

De onder de nummers [NUMMER] genoemde punten moeten op een termijn van [TERMIJN] worden uitgevoerd.

4.3 Adviezen FG en betrokkenen

Advies Functionaris Gegevensbescherming
Leg hieronder het advies van de FG vast.
…

Raadpleging betrokkenen
Zijn de (G)MR/OR of andere betrokkenen geraadpleegd bij de uitvoering van de DPIA, of is de (concept) DPIA gedeeld met de betrokkenen? Zo nee, beschrijf hieronder waarom niet. Zo ja, beschrijf hieronder de input van de betrokkenen.
…

Herziening DPIA
Wanneer wordt de DPIA-rapportage herzien of heroverwogen? *Advies: Herhaal de DPIA om de drie jaar of bij grote wijzigingen in processen of systemen*
…

5. VERKLARING ONDERWIJSINSTELLING

Op basis van het onderzoek dat in het kader van de centrale DPIA en DTIA, alsmede de lokale DPIA is uitgevoerd, zijn de gevolgen voor de rechten en vrijheden van deze betrokkenen door de verwerking van persoonsgegevens van leerlingen en medewerkers in Google Workspace for Education [en ChromeOS en Chromebrowser op beheerde chromebooks]- na toepassing van risico-mitigerende maatregelen – in [onvoldoende/voldoende] mate beheerst.

Deze conclusie is of wordt anders als de in deze lokale DPIA genoemde maatregelen niet of onvoldoende worden uitgevoerd.

De genomen en te nemen maatregelen, waarborgen, veiligheidsmaatregelen en mechanismen die binnen Google Workspace for Education de bescherming van persoonsgegevens garanderen, zijn [onvoldoende/voldoende] gericht op het beperken van de risico's voor de rechten en vrijheden van betrokkenen.

Er is [wel/niet] gebleken van hoge risico's voor de rechten en vrijheden van betrokkenen die moet leiden tot een 'voorafgaande raadpleging' zoals omschreven in artikel 36 AVG.

De het bestuur (bevoegd gezag) van [NAAM ONDERWIJSINSTELLING], overwegende de conclusies en aanbevelingen, verklaart hierbij:

- kennis te hebben genomen van inhoud van deze organisatie-specifieke DPIA;
- kennis te hebben genomen van de door SIVON en SURF uitgevoerde centrale DPIA, DTIA en onderzoek ChromeOS en Chrome-browser, en de door hen gevoerde onderhandelingsresultaten;
- de - in dit rapport - vermelde (rest)risico's te aanvaarden;
- in te stemmen met de uitvoering van de in de rapportage genomen beheersmaatregelen;
- opdracht te geven voor het uitvoeren van de aanbevolen beheersmaatregelen op de daarbij genoemde termijnen;
- deze DPIA na een periode van <termijn> te laten herzien of eerder indien nodig;
- wel / geen voorafgaande raadpleging bij de Autoriteit Persoonsgegevens in te dienen;
- het DPIA-team decharge te verlenen.

EN BESLUIT - NA HEROVERWEGING - HET GEBRUIK VAN [GOOGLE WORKSPACE FOR EDUCATION EN/OF CHROMEOS en CHROME-BROWSER OP BEHEERDE CHROMEBOOKS] [WEL/NIET] TE CONTINUEREN.

Naam onderwijsinstelling:

Naam bestuurder(s):

Plaats:

Datum:

Ondertekening:

BIJLAGE 1: Maatregelen Google Workspace for Education

Technische handleiding voor Google Workspace for Education v3.0			
Par.	**Beschrijving**	Maatregel genomen J/N	Plan-ning
Algemene adviezen en informatie			
2.4	Doorgifte van persoonsgegevens naar derde landen: neem op deze pagina kennis van de subverwerkers van Google: https://workspace.google.com/terms/subprocessors.html		
2.5	Lees hier voor neer informatie over privacy: https://www.google.com/chrome/privacy/whitepaper.html en https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf Toelichting SIVON op tooling Google: https://sivon.nl/uitleg-transparantie-gegevensverwerkingen-google-workspace-for-education/		
2.6	Scope Google Workspace for Education: alleen gebruik “Core services” is toegestaan onder de overeenkomst met Google. Bij gebruik van andere, additionele services is Google en niet de onderwijsinstelling de verwerkingsverantwoordelijke. https://workspace.google.com/intl/en/terms/user_features/ Zet aanvullende Google-services uit: https://support.google.com/a/answer/181865#zippy=%2Cservices-aan--of-uitzetten-voor-gebruikers		
Overzicht maatregelen			
3.2	Maatregelen betreffende gebruikersaccounts		
3.3	Maatregelen betreffende dataminimalisatie in producten en functionaliteiten		
3.4	Individuele maatregelen en instructies		
Centrale beheeropties mogelijk maken			
4.1	Onder beheer plaatsen van Chromebooks en Chromebrowsers		
4.2	Chromebooks onder beheer brengen		
4.3	Chromebook beheerde gastsessie		
4.4	Chromebrowsers onder beheer brengen		
4.5	Instellingen op het besturingssysteem via groepsbeleid		
Instellingen in de Admin console			
5.1	Google Workspace als K-12 instellen		
5.2	Gebruikersnamen in email adres (advies pseudonimiseren)		
5.3	Gebruikersprofielen		
5.4	Geografische locatie dataopslag		
5.5	Aanvullende Google diensten (Additional Services)		
5.6	Google Workspace Marketplace-apps		
5.7	Nieuwe Google producten		
5.8	Spellingcontrole en Spellingcontrole Webservice		
5.9	Chrome synchronisatie uitschakelen		
5.10	Automatische vertaling websites uitzetten		
5.11	Geolocatie uitzetten		
5.12	Gebruikersfeedback niet toestaan		
5.13	Rapportage van statistieken: turn off		

5.14	Nieuw Tabblad		
5.15	Search suggested service (omnibox)		
5.16	Inloggen op secundaire accounts		
5.17	Cookies beleid		
5.18	Systeemrapportages van bezochte pagina's		
5.19	Chrome Cleanup		
Individuele instellingen en instructies			
6.1	Advertentiepersonalisatie (indien K-12 instelling niet geactiveerd is)		
6.2	YouTube video embedding		
6.3	Gebruik van Chrome browser		
Gebruik Google niet als zoekmachine			
7.1	Gebruik een advertentie- en/of tracking blocker		
7.2	Gebruik geen privacygevoelige informatie in file en folder namen (gebruikersinstructie)		
Data Transfer Impact Assesment			
8.1	Data regions. *Let op: dit is niet mogelijk in de gratis versie Google Workspace for Education fundamental, een betaalde licentie is vereist*		
8.2	Overweging toepassen Client Side Encryption		
Beveiligingsinstellingen			
	Overweeg de door Google aanbevolen beveiligingsinstellingen te nemen: https://sivon.nl/wp-content/uploads/2022/06/Beveiliging-Google-Workspace.pdf		

Toelichting comply or explain (toelichting bij afwijking van het advies): zie paragraaf 3.2.2 voor een motivering.

BIJLAGE 2: Maatregelen ChromeOS en Chromebrowser op beheerde chromebooks

Handleiding Google ChromeOS en Chrome-browser 2024			
Hoofd-stuk	**Beschrijving**	Maatregel genomen J/N	Planning
2	**Sluit verwerkersovereenkomst ChromeOS af (Data Processor Mode)**		
3	**Schaf Chrome Education Upgrade aan voor chromebooks (voor de levensduur van ieder chromebook)**		
4	**Privacy instellingen voor ChromeOS en Chrome browser**		
	Zet 'optional services' uit		
	Gebruik altijd K-12 settings		
	Zet de Chrome Web Store uit		
	Zet de Google Play uit		
	Zet ad personalisatie uit. Voor K-12 is dit de default waarde		
	Verstuur geen "crash report" naar Google		
	Overweeg "Safe Sites" uit te zetten en een andere filter functie te implementeren		
5	**Eindgebruikers instellingen**		
	Switch off Privacy Sandbox.		
	Zet advertentieonderwerpen uit		
	Zet door sites voorgestelde advertenties uit		
	Zet advertentiemeting uit		
	Gebruik Chrome Sync encryptie		
6	**Gebruik privacy vriendelijke browsers settings**		
	'Niet bijhouden' uitschakelen (do not track) en disable website preloading		

Toelichting comply or explain (toelichting bij afwijking van het advies): zie paragraaf 3.2.2 voor een motivering.