Handreiking *lokale* DPIA

Google Workspace for Education

DPIA Workspace for Education voor schoolbesturen gebaseerd op landelijke DPIA en verificatie SURF en SIVON

Versie 2.0 (juli 2023)

Inhoudsopgave

1. Inleiding

1.1 Algemeen

In 2021 is er een privacyonderzoek uitgevoerd op Workspace for Education (in 2021 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 SCHOOLBESTUUR] 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).

SIVON en SURF concluderen[2] nu na grondig onderzoek dat scholen Google Workspace voorlopig **kunnen blijven gebruiken**. Dit betekent dat we op onze scholen gebruik kunnen blijven maken van Google Workspace for Education.

De afspraken die zijn gemaakt met Google, gelden ook voor de scholen van [NAAM SCHOOLBESTUUR]. Dat betekent onder andere dat de standaard voorwaarden van Google niet van toepassing zijn, maar dat aanvullende voorwaarden[3] gelden. Daarnaast hebben we ook de gewijzigde contractvoorwaarden geaccepteerd.

1.2 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:

> *(...) Onderwijsinstellingen die onvoldoende maatregelen hebben getroffen dienen bij de inzet van Google G Suite for Education gebruik te maken van deze door SURF en SIVON gemaakte afspraken, eventuele aanvullende maatregelen treffen en vast te stellen of er bij de onderwijsinstelling mogelijk sprake is van additionele risico's ten opzichte van de DPIA.*

[1] https://sivon.nl/2021/07/akkoord-onderwijs-met-google-over-privacyrisicos/
[2] https://sivon.nl/2023/07/privacyrisicos-uit-dpia-van-2021-google-workspace-for-education-voldoende-opgelost/
[3] https://services.google.com/fh/files/misc/gcpnaddendum_jan_23_nl.pdf

Onderwijsinstellingen dienen zelf vast te stellen of er in hun specifieke situatie sprake is van additionele risico's die in de weg staan aan het gebruik van Google G Suite for Education,(...). [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 zullen als verwerkingsverantwoordelijke volgens de AVG zelf een risicoafweging moeten uitvoeren. 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 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.

1.3 Handreiking lokale DPIA: eigen risicoafweging maken

Deze handreiking helpt onderwijsinstellingen om zelf te bepalen of de nieuwe afspraken en verificatie in 2023, de persoonsgegevens van leerlingen, hun ouders en medewerkers voldoende beschermen conform de AVG. Hierbij gaat het niet alleen om het afwegen van de risico's die volgen uit uitgevoerde en aangepaste DPIA, maar ook of er in de specifieke situatie van uw onderwijsinstellingen sprake is van additionele risico's die gemitigeerd moeten worden.

De handreiking is gesplitst in twee stappen:

1. Gegevensverwerkingsanalyse: een beschrijving van de gegevensverwerking voorzien van een beoordeling van de noodzaak en evenredigheid van de verwerkingen als het gaat om de doeleinden.
2. Risicoanalyse: de weging van de risico's (voor de betrokken personen) en de te nemen maatregelen om de privacyrisico's te beperken.

Neem beide hoofdstukken samen met de betrokkenen uit uw instelling door. Op deze wijze kunt u de analyse en besluitvorming over de risico's van het gebruik van Google Services voor uw specifieke instelling vastleggen.

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

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

[4] Autoriteit Persoonsgegevens, Advies: Google G Suite for Education; z2021-08230, 31 mei 2021, p. 6.

Deze handreiking wordt gebruikt in samenhang met de volgende documentatie:

1. Workspace for Education (Online) agreement (aanpassingen overeenkomst, dd. augustus 2021)[5]
2. DPIA G Suite / Google Workspace maart 2021[6]
3. Update on Google Workspace for Education DPIA, SURF and SIVON, dd 2 augustus 2021[7]
4. Technische handleiding voor Google Workspace for Education (augustus 2021)[8]
5. Verification report Google remediation measures Workspace for Education, 15 juni 2023[9]

[5] Deze overeenkomst wordt separaat door Google aan onderwijsinstellingen aangeboden aan de 'administrator' van Google Workspace for Education binnen de school.
[6] https://slmmicrosoftrijk.nl/wp-content/uploads/2021/03/Google-Workspace-DPIA-for-Dutch-DPA-v18-Feb-2021.pdf
[7] https://sivon.nl/wp-content/uploads/2022/07/Update-DPIA-report-Google-Workspace-for-Education-2-augustus-2021.pdf
[8] https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/Kennisnet-Technische-handleiding-Google-Workspace-for-Education.pdf
[9] https://sivon.nl/dpia-google-workspace/

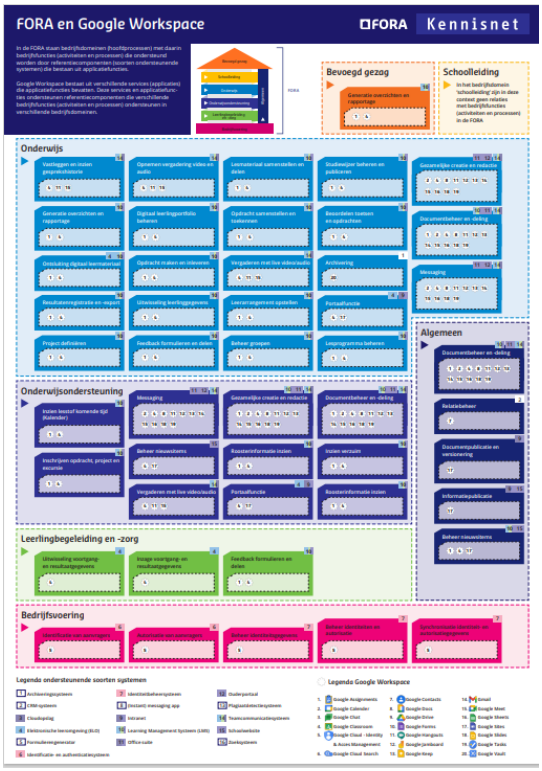
2. Gegevensverwerkingsanalyse

De gegevensverwerkingsanalyse start met het inventariseren voor welke doeleinden gegevens worden verwerkt bij het gebruik van Google services. Dit doet u aan de hand van de processen die hiermee worden ondersteund. Vervolgens dient u een beoordeling te maken over de rechtmatigheid van de gegevensverwerking. Hiermee wordt bovendien inzichtelijk of er aanvullende maatregelen nodig zijn om te voldoen aan de vereisten van rechtmatigheid.

Betrek bij het opstellen van de gegevensverwerkingsanalyse de personen binnen de onderwijsinstelling die een goed beeld hebben van de processen en data die in verschillende Google services worden verwerkt, inclusief de gegevenskoppelingen.

2.1 Processen

De basis voor deze analyse zijn procesbeschrijvingen, waarbij gebruik is gemaakt van de bedrijfsfuncties die zijn beschreven in de FORA[10].



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:

[10] 8733_Figuur_Toepassingen_Google_Workspace-FORA_FASE_2_-_2022_01.pdf (wikixl.nl)

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

2.2 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:		
	…	☐
	…	☐

2.3 Persoonsgegevens

Voor het in gebruik nemen van een account in Google Workspace for Education 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.

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 (augustus 2021)*[11] 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
	(Fictieve) achternaam	
	Wachtwoord	
	E-mailadres (school)	

[11] https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/Kennisnet-Technische-handleiding-Google-Workspace-for-Education.pdf

		Workspace for Education
Leerling, medewerker	Diagnostische gegevens, zoals log- en monitoringsgegevens, metadata	Zie DPIA Google Workspace for Education d.d. 12 maart 2021
	IP-adres	
	Persoonsgegevens gebruikers (*Customer data*) in bestanden	
…	Andere persoonsgegevens, namelijk: … … …	…

2.4 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.

Geef vervolgens aan of binnen het proces aan het vereiste van dataminimalisatie is voldaan: 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.

Geef tot slot aan of er is voldaan 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 de andere doeleinden in.

3. Risicoanalyse

Om een risicoanalyse uit te voeren neemt u eerst 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. Tenslotte analyseert u uw instelling-specifieke risico's en eventuele mitigerende maatregelen.

3.1 Overzicht centraal vastgestelde risico's en maatregelen

3.1.1 Centraal vastgestelde risico's en mitigerende maatregelen Google

In de centrale *DPIA Google Workspace for Education d.d. 12 maart 2021* zijn hoge risico's vastgesteld. Deze zijn besproken met Google waarna Google toezeggingen heeft gedaan om deze risico's te beperken. Dat is opgenomen in het Update DPIA Report Workspace for Education DPIA, SURF and SIVON, dd 2 augustus 2021[12]. Hierbij hoort een technische handleiding (augustus 2021)[13] met maatregelen om risico's te beperken. In *het Verification report Google remediation measures Workspace for Education* (15 juni 2023)[14] wordt de stand van zaken beschreven en welke maatregelen de hoge privacyrisico's beperken.

Het gaat om de risico's

1. Gebrek aan doelbinding voor klantgegevens.
2. Gebrek aan doelbinding voor diagnostische (meta) gegevens waarvoor Google zichzelf als verwerkingsverantwoordelijke beschouwt.
3. Gebrek aan transparantie over de klantgegevens.
4. Gebrek aan transparantie over de diagnostische (meta) gegevens.
5. Geen juridische grondslag voor onderwijsinstellingen en Google.
6. Gebrek aan mogelijkheid voor beheerders om privacy-vriendelijke instellingen centraal te regelen.
7. Gebrek aan controle over (sub)verwerkers en derde partijen die toegang hebben tot m.n. de diagnostische gegevens.
8. Betrokkenen krijgen geen inzage in de diagnostische (meta) persoonsgegevens die Google verwerkt.
9. De doorgifte van gegevens naar landen buiten de EER (waaronder de VS) brengt het risico met zich mee dat persoonsgegevens onrechtmatige verwerkt worden.

Ten aanzien van risico 9, doorgifte van persoonsgegevens buiten de EER, voeren SURF en SIVON een data transfer impact assessment (DTIA) uit. Deze wordt in het najaar 2023 verwacht. De DPIA (Update DPIA Report 2021 en Verificatie report 2023) gaan uit van de betaalde versie van Google Workspace for Education omdat deze opties voor (geavanceerde) gegevensbescherming (beveiligingscentrum), beheer van devices (Chromebooks), gebruik logboeken, en opslag van data binnen de Europese Unie kent. De gratis versie[15] kent deze opties niet waarmee niet de juiste privacyinstellingen en logboeken kunnen worden

[12] https://sivon.nl/wp-content/uploads/2022/07/Update-DPIA-report-Google-Workspace-for-Education-2-augustus-2021.pdf
[13] https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/Kennisnet-Technische-handleiding-Google-Workspace-for-Education.pdf
[14] https://sivon.nl/dpia-google-workspace/
[15] Workspace for Education Fundamentals: https://edu.google.com/intl/ALL_nl/workspace-for-education/editions/compare-editions/

gebruikt. Onderwijsinstellingen die de gratis versie gebruiken, kunnen overstappen op de betaalde versie of deze (overweging voor) overstap maken bij het bekend worden van de uitkomsten van de DTIA.

Het nummer in onderstaande tabel, verwijst naar de voornoemde risico's zoals benoemd in het Update DPIA report uit 2021.

Risico nr.	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 Workspace for Education (online) agreement (Privacy Amendement).
		Google zal geen Persoonsgegevens van Klanten en/of Servicegegevens verwerken voor advertentiedoeleinden of voor profilering, gegevensanalyse en marktonderzoek.	Risico beperkt door contractuele maatregelen in Workspace for Education (online) agreement (Privacy Amendement).
		7 geïdentificeerde doeleinden waarvoor Google als onafhankelijke gegevensbeheerder Diagnostische gegevens verder mag verwerken. 1. facturering en accountbeheer en klantrelatiebeheer en bijbehorende 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 de 17 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.	*** Opmerking**: onjuiste informatie Google in het voorgestelde nieuwe GCPN addendum over overeengekomen doeleinden, "*Wij gebruiken Servicegegevens om u en onze klanten informatie te verstrekken over nieuwe of gerelateerde producten en functies met betrekking tot Cloudservices waarop onze klanten zich abonneren.*" Dit is een laag risico omdat de voorwaarden in het Workspace for Education (online) agreement (Privacy Amendement) prevaleren boven alle 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*

Risico nr.	Risico	Overeengekomen verzachtende maatregel Google	Feitelijke maatstaf
			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 Workspace for Education (online) agreement (Privacy Amendement).
		In de raamovereenkomst is vastgelegd hoe Google omgaat met *knevelbevelen* wanneer het bevel wordt gegeven om Inhoud en diagnostische gegevens vrij te geven aan rechtshandhavingsinstanties.	In Workspace for Education (online) agreement (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. *** Opmerking** door te kiezen voor **K12**, worden privacy-instellingen automatisch ingesteld en afgedwongen.
3, 4, 7[16]	**Gebrek aan transparantie Klant- en servicegegevens**	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 (waaronder mogelijk ook Content Data). De toegangsperiode beslaat alleen de laatste 24 uur, vanwege de lange hersteltijd.
		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 soorten 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 Statement. Hierin worden de 3 criteria beschreven die Google hanteert om Servicegegevens langer dan een jaar te bewaren. Dit zijn: 1. *Beveiliging, preventie van fraude en misbruik,* 2. *Voldoen aan wettelijke of regelgevende vereisten en* 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	Google heeft de informatie over zijn subverwerkers en filialen uitgebreid, welke persoonlijke gegevens zij voor welke doeleinden kunnen inzien.

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

Risico nr.	Risico	Overeengekomen verzachtende maatregel Google	Feitelijke maatstaf
		Diagnostische gegevens. Google zal het volgende specificeren o volledige naam van de entiteit, o relevante dienst(en), o locatie(s) waar de gegevens worden verwerkt, o activiteit (d.w.z. wat doet de subprocessor, o of de subverwerker Servicegegevens verwerkt in tijdelijke, persoonlijke en/of archieflogboeken.	**OUT OF SCOPE** De lijst met subverwerkers bevat bedrijven en filialen in derde landen. Google werkt samen met SURF en SIVON aan de lopende DTIA om de risico's van overdracht naar derde landen te beoordelen.
		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 maken in een kennisgeving voor eindgebruikers.	De pop-up is verbeterd en gepersonaliseerd. De relevante juridische informatie is echter niet permanent beschikbaar via het inlog- of Google-accountmenu. Google heeft toegezegd de verwijzingen in de accountinformatie voor 25 november 2025 opnieuw vorm te geven. Google zal in december 2023 een gedetailleerde tijdlijn voor dit redesign aan SURF en SIVON presenteren.
		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 Google Cloud 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 minimalistische uitleg.
		Google zal de beschikbaarheid van admin-auditlogs uitbreiden naar alle Core Services.	Google levert veel meer auditlogs, in overeenstemming met het verbeterplan voor zover getest.
5, 6	**Geen wettelijke grond voor Google en scholen/universiteiten + Ontbreke**	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 Content data in telemetriegebeurtenissen over Spelling- en grammaticatelemetriegebeurtenissen uit in een apart onderwerp op de nieuwe DIT-informatiepagina, onder *Spelling- en grammaticasuggesties*.

Risico nr.	Risico	Overeengekomen verzachtende maatregel Google	Feitelijke maatstaf
	nde privacycontroles		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 Workspace for Education (online) agreement en 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. Overheidsorganisaties wordt geadviseerd hun werknemers te waarschuwen geen gebruik te maken van Feedback, om te voorkomen dat ze medeverantwoordelijk worden voor de verwerking.	Google is gegevensverwerker voor de levering van TSS volgens Privacywijziging. De verwerking van feedbackgegevens is een overeengekomen legitiem bedrijfsdoel.
		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 eindgebruikers om hun eigen 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 (zie 2 rijen hieronder).
		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' (super administrators) 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 op basis van 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*.

Risico nr.	Risico	Overeengekomen verzachtende maatregel Google	Feitelijke maatstaf
		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		NIET VAN TOEPASSING: De risico's van overdracht worden apart beoordeeld in de lopende DTIA.

Op basis van de bovenstaande tabel en de overige beschikbare documentatie zoals hieronder genoemd, beoordeelt u voor uw onderwijsinstelling of de beschreven maatregelen voldoende zijn om de hoge risico's van het gebruik van Google Workspace for Education weg te nemen.

Zijn de door Google 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:	
Workspace for Education (Online) agreement (aanpassingen overeenkomst, verzonden 9 augustus 2021)	
DPIA G Suite for Education d.d. 12 maart 2021	
Update on Google Workspace for Education DPIA, SURF and SIVON, 2 augustus 2021	
Handleiding technische maatregelen (augustus 2021)	
Verification report Google remediation measures Workspace for Education, 15 juni 2023	
Advies van de Functionaris Gegevensbescherming van [NAAM SCHOOLBESTUUR] d.d. <datum>	
Raadpleging betrokkenen ((G)MR, Studentenraad en/of OR) d.d. <datum>	

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

Indien het antwoord op bovenstaande vraag 'Nee' is, is de conclusie voor uw onderwijsinstelling dat er geen gebruik gemaakt kan worden van Google Workspace for Education. U hoeft het resterende deel van deze DPIA in dat geval niet uit te voeren en u kunt direct verder naar de Verklaring schoolbestuur in hoofdstuk 5, inhoudende dat Google Workspace for Education niet (verder) gebruikt zal worden.

3.1.2 Centraal vastgestelde maatregelen onderwijsinstelling

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 uw 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 (augustus 2021)[17] zijn instellingen opgenomen die onderwijsinstellingen zelf moeten doorvoeren om de privacyrisico's te mitigeren.

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 *Handleiding technische maatregelen*, 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.

3.1.3 Aanbevelingen beveiliging

Bij het veilig en verantwoord omgaan met persoonsgegevens, horen ook de juiste beveiligingsinstellingen. SIVON heeft in samenwerking met Google een aantal *aanbevelingen* voor beveiligingsinstellingen[18] opgesteld voor Google Workspace for Education. Overweeg om deze aanbevolen instellingen te gebruiken.

3.2 Inventarisatie eventuele organisatie-specifieke risico's + 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 een centrale DPIA 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 3.1 beschreven risico's? 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

[17] https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/Kennisnet-Technische-handleiding-Google-Workspace-for-Education.pdf
[18] https://sivon.nl/wp-content/uploads/2022/06/Beveiliging-Google-Workspace.pdf

- 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.

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.

[De volgende mogelijke risico's (impact op de rechten en vrijheden van betrokkenen) en eventuele schade, weeg hierbij mogelijk risico's op het gebied van:

- onvermogen om rechten uit te oefenen (inclusief maar niet beperkt tot privacyrechten);
- onvermogen om toegang te krijgen tot diensten of kansen;
- verlies van controle over het gebruik van persoonsgegevens;
- discriminatie;
- identiteitsdiefstal of fraude;
- financieel verlies;
- reputatieschade;
- verlies van vertrouwelijkheid;
- heridentificatie van gepseudonimiseerde gegevens; of
- elk ander significant economisch of sociaal nadeel
- gevolgen en risico's voor de beveiliging van [SYSTEEM].]

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. Eindconclusie onderwijsinstelling

4.1 Afweging risico's

De laatste stap die in deze organisatie-specifieke DPIA wordt genomen is het inventariseren van de restrisico's. Deze risico's ontstaan aan de ene kant omdat een onderwijsinstelling de centraal vastgestelde maatregelen niet neemt (of kan nemen) en anderzijds omdat er organisatie-specifieke restrisico's zijn vastgesteld die niet door maatregelen kunnen worden weggenomen. Voor deze inventarisatie gaat u eerst terug naar de tabel die u in paragraaf 3.1.2 heeft ingevuld. Zijn er maatregelen beschreven in die tabel die uw onderwijsinstelling niet kan of wil nemen? En zo ja, welk risico blijft daardoor bestaan?

Daarna inventariseert u in paragraaf 3.2 of en zo ja, welke restrisico's zijn beschreven en wat hun classificatie is.

Vraag 1 **Zijn of worden alle maatregelen zoals benoemd in paragraaf 3.1.2 binnen een voorzienbare termijn door uw onderwijsinstelling uitgevoerd?** **Ja/nee** **Indien 'Ja', ga door naar vraag 2.** **Indien 'Nee', neem hieronder de niet uitgevoerde maatregel en bijbehorend restrisico met classificatie over.**		
Niet uitgevoerde maatregel	Bijbehorend restrisico	Classificatie restrisico (laag, midden, hoog)
…		
…		
…		
Vraag 2 **Zijn er in de tabel in paragraaf 3.2 – andere dan lage - restrisico's beschreven?** **Ja/nee** **Indien 'ja', geef hieronder aan welk(e) risico's het betreft en wat de classificatie is)**		
Beschreven restrisico		Classificatie restrisico (laag, midden, hoog)
…		
…		
…		

Als er in bovenstaande tabel **hoge** restrisico's zijn opgenomen, dan mag u op grond van de AVG Google Workspace for Education **niet** gebruiken voor de daarbij behorende doeleinden. Het bestuur van uw onderwijsinstelling kan twee besluiten nemen:

1. Google Workspace for Education niet gebruiken.
2. Een voorlopige raadpleging indienen bij de Autoriteit Persoonsgegevens op basis van artikel 36 AVG.

Wanneer er geen, lage of gemiddelde restrisico's zijn vastgesteld dan maakt het bestuur van de onderwijsinstelling een gemotiveerde afweging om Google Workspace for Education - al dan niet - te blijven gebruiken. Hierbij accepteert het bestuur actief de geconstateerde (rest)risico's.

Bij het besluit wordt het advies van de functionaris voor gegevensbescherming (FG) van de onderwijsinstelling betrokken. Daarnaast is het aan te bevelen om ook de betrokkenen om hun mening te vragen over de bevindingen bij deze DPIA. Denk bijvoorbeeld aan de (G)MR of OR en de leerlingen- of studentenraad. Dit kan vervolgens worden meegenomen bij het uiteindelijke besluit van het bestuur van de onderwijsinstelling. Het advies van de FG en de input van de betrokkenen wordt hieronder in het rapport opgenomen.

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***
…

4.2 Communicatie

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[19].

Het is belangrijk voor de school om ook zelf betrokkenen te informeren over de uitkomsten van de DPIA. SIVON heeft voorbeeldbrieven[20] gemaakt voor leerlingen, hun ouders, medewerkers en de GRM en Raad van Toezicht.

[19] https://services.google.com/fh/files/misc/gcpnaddendum_jan_23_nl.pdf
[20] https://sivon.nl/alles-over-de-dpias-op-google-workspace-chromeos/

5. VERKLARING SCHOOLBESTUUR

Op basis van het onderzoek dat in het kader van de centrale DPIA, alsmede de lokale DPIA is uitgevoerd, zijn de gevolgen voor de rechten en vrijheden van deze betrokkenen door de verwerking van persoonsgegevens van onderwijsdeelnemers en medewerkers in Google Workspace for Eduation - 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 verwerkingsverantwoordelijke van [naam schoolbestuur], overwegende de conclusies en aanbevelingen, verklaart hierbij:

- kennis te hebben genomen van inhoud van dit organisatie-specifieke DPIA
- kennis te hebben genomen van het namens SURF en SIVON uitgevoerde centrale DPIA (Update DPIA Report en Verificatie Report) en de door hen gevoerde onderhandelingsresultaten
- de - in dit rapport - vermelde restrisico'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
- dit 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 **[WEL/NIET]** TE CONTINUEREN.

Naam onderwijsinstelling:

Naam bestuurder(s):

Plaats:

Datum:

Ondertekening:

Colofon

Handreiking lokale DPIA Google Workspace for Education

Datum van uitgave
5 augustus 2021 (versie 1.0), update 13 juli 2023 (versie 2.0)

Auteurs
Versie 1.0: Ymkje Koster (Kennisnet) en Job Vos (SIVON)
Versie 2.0: Hans-Peter Ligthart en Job Vos (SIVON)

Bij deze DPIA is gebruik gemaakt van 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. **Kennisnet** bevordert 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.

sivon.nl
kennisnet.nl