Handreiking onderwijsspecifieke DPIA Google Workspace for Education

Augustus 2021

Inhoudsopgave

1. Inleiding 3
2. Gegevensverwerkingsanalyse 5
2.1 Processen 5
2.2 Doeleinden verwerkingen persoonsgegevens 7
2.3 Persoonsgegevens 8
2.4 Beoordeling van de rechtmatigheid 9
3. Risicoanalyse 13
3.1 Overzicht centraal vastgestelde risico's en maatregelen 13
3.1.1 Centraal vastgestelde risico's 13
3.1.2 Centraal vastgestelde maatregelen Google 13
3.1.3 Centraal vastgestelde maatregelen onderwijsinstelling 17
3.2 Inventarisatie eventuele organisatie-specifieke risico's + maatregelen 17
4. Eindconclusie onderwijsinstelling 20
5. VERKLARING SCHOOLBESTUUR (verwerkingsverantwoordelijke) 22
Bijlage – Tabel hoge risico's en mitigerende maatregelen Google 23
Colofon 24

1. Inleiding

Met de onderhandelingen die SURF, SIVON en SLM Rijk met Google voeren, 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 er is meer nodig voordat onderwijsinstellingen kunnen besluiten of zij het gebruik van Google Workspace for Education willen voortzetten of starten. Zij zullen – als verwerkingsverantwoordelijke volgens de AVG – zelf een heroverweging van risico's moeten uitvoeren die eerder zijn vastgelegd in de landelijke DPIA. Daarnaast moeten zij nagaan of het eigen gebruik van Google Workspace for Education nog andere privacyrisico's oplevert die moeten worden weggenomen.

Dit volgt uit de Algemene Verordening Gegevensbescherming (AVG) en is door de Autoriteit Persoonsgegevens (AP) nog eens benadrukt in het advies over het gebruik van Google Workspace for Education d.d. 31 mei 2021:

> *(...) 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. 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,(...).* [1]

Deze handreiking helpt onderwijsinstellingen om te bepalen of de nieuwe afspraken de persoonsgegevens 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.

In de handreiking is de informatie die is verzameld bij het uitvoeren van de centrale DPIA op Google Workspace for Education zoveel mogelijk opgenomen. Onderwijsinstellingen bepalen op basis daarvan zelf welke beschreven verwerkingen, risico's en maatregelen op de eigen situatie van toepassing zijn. Ontbrekende verwerkingen, risico's en maatregelen voegen ze toe.
Op basis van die informatie stelt het schoolbestuur vast welke (additionele) risico's bij het gebruik van Google Workspace for Education op de eigen situatie van toepassing zijn, welke maatregelen nodig zijn om die risico's weg te nemen en welke restrisico's overblijven. Het bestuur weegt deze restrisico's af en besluit op basis van die weging over (voortzetting van) het gebruik van Google Workspace for Education.

De handreiking is gesplitst in twee stappen:

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

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.

Deze handreiking wordt gebruikt in samenhang met de volgende documentatie:
1. Workspace for Education (Online) agreement (aanpassingen overeenkomst, dd. augustus 2021)[2]
2. DPIA G Suite for Education d.d. 12 maart 2021
3. Update on Google Workspace for Education DPIA, SURF and SIVON, dd 2 augustus 2021
4. Technische handleiding voor Google Workspace for Education (augustus 2021) [3]

[2] Deze overeenkomst wordt separaat door Google aan onderwijsinstellingen aangeboden. Informatie hierover wordt bekend gemaakt door SURF en SIVON.
[3] De DPIA, Update en Handleiding zijn te vinden op websites van SIVON en SURF.

2. Gegevensverwerkingsanalyse

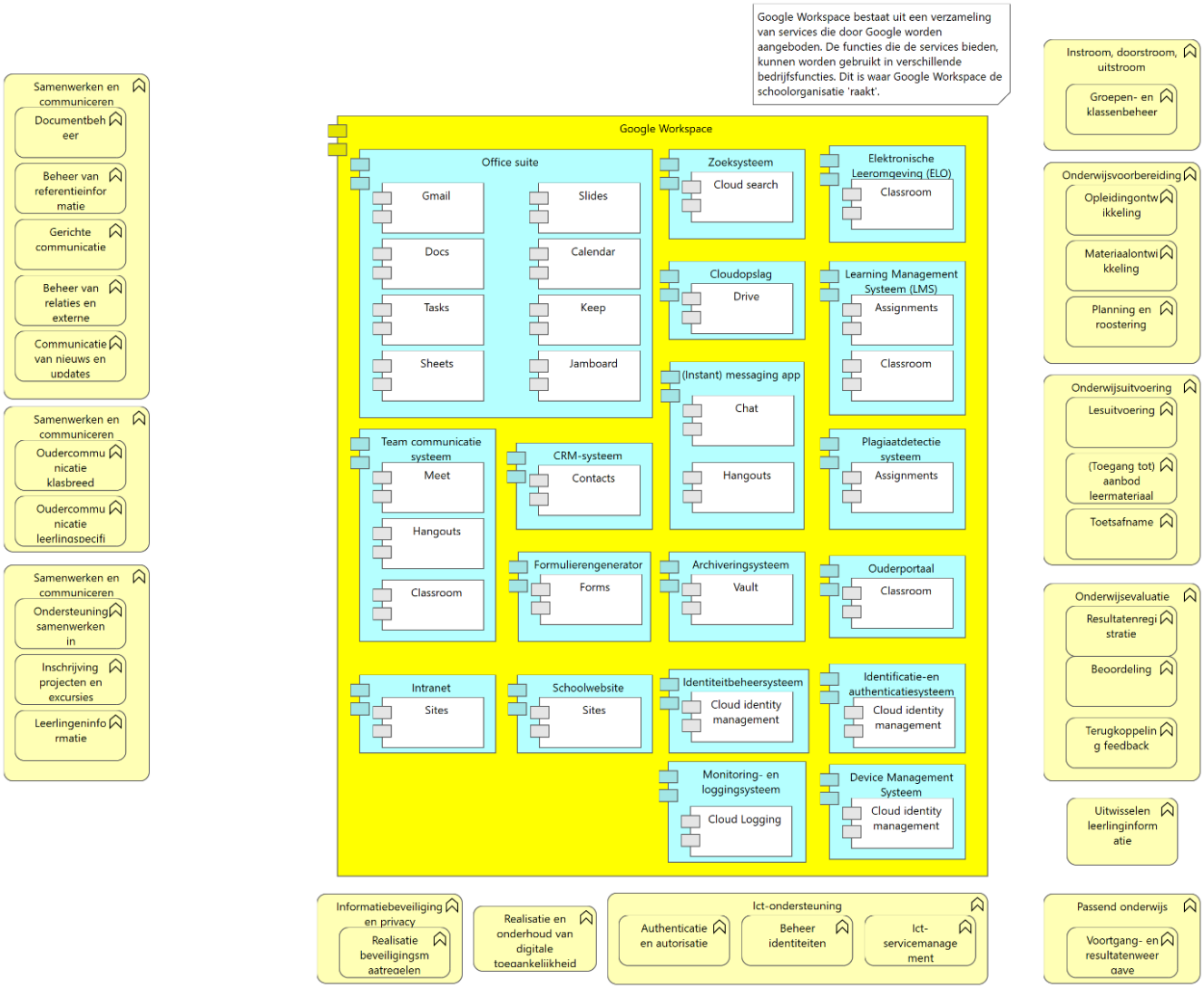
De gegevensverwerkingsanalyse start met het inventariseren voor welke doeleinden gegevens worden verwerkt bij het gebruik van Google services. Dit doet u aan de hand van de processen die hiermee worden ondersteund. Vervolgens dient u een beoordeling te maken over de rechtmatigheid van de gegevensverwerking. 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 (zie afbeelding op de volgende pagina).

Deze afbeelding biedt onderwijsinstelling ondersteuning om in kaart te brengen bij welke processen en voor welke bedrijfsfuncties gebruik wordt gemaakt van Google services.



Afb. Kennisnet-FORA, Bedrijfsfuncties Google Workspace – Google Services d.d. 21 juni 2021

Wilt u meer informatie over de bedrijfsfuncties? Dit vindt u op de website van de FORA.
Instellingen voor hoger onderwijs maken gebruik van de HORA.

Is bovenstaande plaat onvoldoende leesbaar? Bekijk of download dan de afbeelding via deze link.

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:		

	...	☐
	...	☐

* De *Update on Google Workspace for Education DPIA* bevat het advies om geen speciale en gevoelige categorieën persoonsgegevens met betrekking tot de leerlingen op te slaan zonder aanvullende maatregelen zoals encryptie. Gebruik hiervoor een aparte tool zoals een LAS, SIS of LVS.

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)*[4] 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 DPIA Google Workspace for Education d.d. 12 maart 2021
	IP-adres	
	Persoonsgegevens gebruikers (*Customer data*) in bestanden	
...	Andere persoonsgegevens, namelijk:	...

[4] Deze handleiding is te vinden op de websites van SIVON en SURF.

	... ...	

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. In de *Update on Google Workspace for Education DPIA* zijn de risico's en maatregelen beschreven en wordt ook aangegeven welke soorten persoonsgegevens van kinderen niet in Google Workspace for Education verwerkt kunnen worden.

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: …

* De *Update on Google Workspace for Education DPIA* bevat het advies om geen speciale en gevoelige categorieën persoonsgegevens met betrekking tot de leerlingen op te slaan zonder aanvullende maatregelen zoals encryptie. Gebruik hiervoor een aparte tool zoals een LAS, SIS of LVS.

** 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.

Wanneer er voor één of meer doeleinden nog niet is voldaan aan de eisen van rechtmatigheid (grondslag, dataminimalisatie en transparantie), dan kunt u hieronder beschrijven op welke wijze en binnen welke termijn u daarvoor maatregelen treft. Deze maatregel(en) neemt u ook over in het overzicht van organisatie-specifieke risico's en te nemen maatregelen in paragraaf 3.2 hieronder.

U kunt hierbij bijvoorbeeld denken aan het aanvullen van uw privacystatement met informatie aan betrokkenen over de verwerkingen of het dichtzetten van velden in een service waar meer persoonsgegevens worden gevraagd dan noodzakelijk voor het doeleinde.

Nog te treffen maatregelen om te voldoen aan de vereisten van rechtmatigheid (grondslag, dataminimalisatie en transparantie)	Termijn waarbinnen maatregel wordt getroffen

N.v.t./ <beschrijving maatregel>*	<datum>
N.v.t./ <beschrijving maatregel>*	<datum>

* Haal door wat niet van toepassing is.

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

In de centrale *DPIA Google Workspace for Education d.d. 12 maart 2021* zijn de volgende 8 hoge risico's vastgesteld:

1. Gebrek aan doelbinding voor klantgegevens.
2. Gebrek aan doelbinding voor diagnostische gegevens waarvoor Google zichzelf als verwerkingsverantwoordelijke beschouwt.
3. Gebrek aan transparantie over de klantgegevens.
4. Gebrek aan transparantie over de diagnostische 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 persoonsgegevens die Google verwerkt.

Daarnaast zijn de volgende lage risico's vastgesteld:

1. De doorgifte van gegevens naar landen buiten de EER (waaronder de VS) brengt het risico met zich mee dat persoonsgegevens onrechtmatige verwerkt worden.
2. De mogelijkheid om op basis van loggegevens medewerkers en leerlingen te volgen en beoordelen bij hun werkzaamheden kan een zogenaamd *chilling effect* hebben op medewerkers en leerlingen.
3. Het gebrek aan mogelijkheden om historische diagnostische gegevens van individuele personen te verwijderen brengt het risico met zich mee dat deze gegevens langer worden bewaard dan noodzakelijk.

3.1.2 Centraal vastgestelde maatregelen Google

In de tabel hieronder staan de mitigerende maatregelen die Google moet nemen beschreven. Deze tabel is overgenomen uit de *Update on Google Workspace for Education DPIA*.

No.	Risk	Mitigating measure Google
1	**Lack of purpose limitation Customer Data**	Google will only process Customer Personal Data and Account Data as data processor, for three purposes, when necessary: *1. to provide, maintain and improve the Services and Technical Support Services (TSS) subscribed to by Customer;* *2. to identify, address and fix security threats, risks, bugs and other anomalies*

		3. *to develop, deliver and install updates to the Services subscribed to by Customer (including new functionality related to the Services subscribed to by Customer).*
		Google will not process Customer Personal Data and/or Service Data for Advertising purposes or for profiling, data analytics and market research.
		7 purposes identified for which Google may process Customer Data as independent data controller. 1. billing and account management and customer relationship management and related correspondence with Customers and Customer Administrators; 2. improving and optimizing the performance and core functionality of accessibility, privacy, security and IT infrastructure efficiency of the Cloud Services and TSS; 3. internal reporting, financial reporting, revenue planning, capacity planning and forecast modeling (including product strategy); 4. abuse detection, prevention and protection (such as automatic scanning for matches with identifiers of CSAM, virus scanning and scanning to detect AUP violations); 5. processing of Personal Data in support tickets and support requests ((including corresponding with Customers and Customer Administrators) and any attachments thereto) sent by Administrators to Google; 6. receiving and using Feedback; and 7. complying with legal obligations. For clarity, the rendering of TSS is a processor activity. With regard to content scanning for Child Sexual Abuse Material (CSAM) and reporting 'hits' to NCMEC, Google will comply with applicable regulatory guidance from the EDPB.
		Google assures that machine learning to improve the contents of Spelling and Grammar Data is limited to within the customer's own Enterprise domain.
		Definition of anonymisation included in the privacy amendment, in accordance with WP29 guidance on anonymisation techniques.
		The framework contract specifies how Google deals with *gagging orders* when ordered to disclose Content Data to law enforcement authorities.
2	**Lack of purpose limitation Diagnostic Data**	Google will only process Diagnostic Data as data processor by the start of the new schoolyear for the three purposes mentioned above, when necessary. Google will ensure that the 17 purposes in the Google Cloud Privacy Notice will not apply to the use of Workspace by Dutch schools and universities.
		Google will not process Customer Personal Data and/or Service Data for Advertising purposes or for profiling, data analytics and market research.
		Google will switch the default setting for Ads Personalization to Off for new end users by Q1 2022 (relevant for the use of Additional Services). In the K-12 Workspace for Education version this is already off by default. When schools and universities switch to the K12 setting, Ads Personalization will automatically be switched Off. K-12 end users cannot override this Ads Personalization setting
		Google will provide Dutch educational institutions with a separate 'data processor' version of the Chrome OS and the Chrome browser on Chromebooks, and a separate data processor version of the Chrome browser for managed devices/managed profiles.

		The framework contract specifies how Google deals with *gagging orders* when ordered to disclose Diagnostic Data to law enforcement authorities.
3	**Lack of transparency Customer Data**	Google will develop an inspection tool to provide access for admins to contents of Customer Data in Diagnostic Data (including telemetry data and use of Features), if stored and not immediately scrubbed, by 31 December 2022.
		Google provides a new warning to end users in the Feedback form not to share sensitive data with Google
		Google will show an end user profile picture on the landing page for all Workspace Core Services (both web and mobile) by Q1 2022. This picture will disappear when end user leaves the privacy protected Workspace services.
		Google will make all relevant legal information about the Google Workspace account permanently available in an end user notice by Q1 2022.
		Google has improved its explanation to admins in the Data Protection Implementation Guide that Google processes Account Data as a processor when the Google Account is used in the Core Services.
		Google has not announced measures to provide exhaustive and comprehensible information and visually clarify the difference between the three different spellingcheckers
4	**Lack of transparency Diagnostic Data**	Google will publish a Help Center article detailing categories and purposes of the processing of diagnostic data (including data collected from cloud servers and telemetry events (atoms) from Android and the Chrome OS by Q1 2022.
		Google will expand the availability of admin audit logs to cover all Core Services and Google will develop a Domain Wide Takeout capability to individual user level/org unit level by 31 December 2022.
		Google will provide an inspection tool for admins to inspect the collected telemetry data and data generated on Google's cloud servers by 31 December 2022. Google will show pilot versions to SIVON and SURF during development.
		Google confirmed that all subprocessors that process Diagnostic Data also process Customer Data, and are therefore already included in the list of subprocessors for Customer Data. Google will publish the necessary details per subprocessor about the categories of data, purposes and locations by 1 September 2021.
		Google will make all relevant legal information about the Google Workspace account permanently available in an end user notice by 31 December 2021.
5	**No legal ground for Google and schools/universities**	Google asks pupils and students for consent for the data processing in the Additional Services (in its role as data controller). It is Google's responsibility to obtain valid consent, not the schools' and universities'.
		Google becomes a data processor for the Diagnostic Data, but not for the support tickets with attachments and Feedback Data.Schools and universities are advised not to use these services, to prevent becoming joint controllers.
		With regard to the (separate) legal ground for the reading of cookie and telemetry data from end-user devices, as defined in the ePrivacy Directive, Google will follow regulatory guidance.
6	**Missing privacy controls**	Google enables admins to take 4 of the 6 measures recommended in the initial DPIA report:

		• Google will not re-use of content from *Spelling and Grammar* for machine learning outside of the Enterprise customer's domain • Admins can prohibit the use of Additional Services when logged in with an Education account • Admins can apply policy rules to disable the Enhanced Spellchecker in the Chrome browser, without the separate Chrome Education Upgrade. • Google will change the default setting for new users for Ads Personalization to Off by 31 December 2022 (in Education versions for primary and secondary schools (K-12 schools) it is already off by default). Additionally, Google will publish detailed information about the telemetry events it collects from Workspace, incl. for Android, by Q1 2022.
7	**Lack of control third parties / processors**	Google will provide details about its subprocessors, in particular for the Diagnostic Data, by Q3 2021. Google will specify o full entity name, o relevant Service(s), o location(s) where the data are processed, o activity (i.e. what does the subprocessor do, o whether the subprocessor processes Service Data in temporary, personal and/or archive logs.
8	**No access for data subjects**	Google will publish details by the start of the new school year why it generally cannot provide access to Telemetry Data, Website Data and personal data from Google's SIEM security logs. Google has confirmed it will consider each request under Article 15 GDPR (i.e. no rejection by default)..
		Google will expand the availability of admin audit logs to cover all Core Services and Google will develop a Domain Wide Takeout capability to individual user level/org unit level by 31 December 2022.
		Google will provide an inspection tool for admins to inspect the collected telemetry data and data generated on Google's cloud servers by 31 December 2022. Google will show SURF and SIVON pilot versions during development.
9	**Transfer of personal data to the USA**	Google will offer the new SCCs for transfers outside of the EEA.
		Google will provide reasonable assistance and all information required in order to make a Data Transfer Risk assessment under the SCC in Q3 2021.
		Google will provide detailed information in what Core Services customers can choose to store the Content Data in the EU, and in what Core Services such a choice is not available by Q3 2021.

Gemakshalve is in de bijlage bij dit document een vertaling van de bovenstaande hoge risico's en door Google te nemen mitigerende maatregelen opgenomen.

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)*
Advies van de Functionaris Gegevensbescherming van [naam onderwijsinstelling] 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.

3.1.3 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.

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.

3.2 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
- 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.

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

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 3.1.3 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 3.1.3 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 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.

Bij het besluit wordt het advies van de 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***
…

5. VERKLARING SCHOOLBESTUUR (verwerkingsverantwoordelijke)

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 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 (PLUS) **[WEL/NIET]** TE CONTINUEREN.

Naam onderwijsinstelling:

Naam bestuurder(s):

Plaats:

Datum:

Ondertekening:

Bijlage – Tabel hoge risico's en mitigerende maatregelen Google

Aan de onderstaande officieuze vertaling kunnen geen rechten worden ontleend. De vertaling is alleen bestemd voor intern gebruik.

Deze bijlage wordt op een later tijdstip beschikbaar gesteld via sivon.nl.

Colofon

Handreiking onderwijsspecifieke DPIA Google Workspace for Education

Datum van uitgave
5 augustus 2021

Auteurs
Ymkje Koster (Kennisnet) en Job Vos (SIVON)

Redactie
Juwan Mizouri

Bij deze DPIA is gebruik gemaakt van de Model DPIA voor het po, vo en mbo (Kennisnet/saMBO-ICT).

Over Kennisnet
Goed onderwijs legt de basis voor leven, leren en werken en daagt leerlingen en studenten uit om het beste uit zichzelf te halen. Dat vraagt om onderwijs dat inspeelt op sociale, economische en technologische ontwikkelingen. Kennisnet ondersteunt besturen in het primair onderwijs (po), het voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo) bij een professionele inzet van ict en is voor scholen de gids en bouwer van het ict-fundament.

Kennisnet wordt 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).