



DATA PROTECTION IMPACT ASSESSMENT

Bij het gebruik van Google Workspace for Education

Juni 2022

Inhoud

1	Gegevensverwerkingsanalyse	3
1.1	Inventarisatie doeleinden gegevensverwerking	3
1.2	Beoordeling rechtmatigheid van gegevensverwerking	5
1.3	Maatregelen	7
2	Risicoanalyse.....	8
2.1	Centraal vastgestelde risico's.....	8
2.2	Organisatie-specifieke risico's	13
3	Conclusie onderwijsinstelling	16
3.1	Advies Functionaris Gegevensbescherming	16
3.1.1	Waarnemingen	16
3.1.2	Advies	16
3.2	Raadpleging betrokkenen	17
3.3	Herziening DPIA	17
4	Verklaring schoolbestuur.....	18
5	Bijlagen	19

1 Gegevensverwerkingsanalyse

1.1 Inventarisatie doeleinden gegevensverwerking

Hoofdbedrijfsfunctie	Bedrijfsfunctie/doeleinde	Kruis aan indien van toepassing op onderwijsinstelling	Op welke wijze?
Samenwerken en communiceren medewerkers en extern *	Documentbeheer en -deling	☒	Google Drive
	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 leerlingsspecifiek	☐	
Samenwerken en communiceren leerlingen	Leerlingen informeren over logistieke zaken	☒	Google Drive
	Inschrijving projecten en excursies	☐	
	Ondersteuning samenwerken in leerlingprojecten	☐	
Onderwijs-ondersteuning: instroom, doorstroom, uitstroom *	Groepen en klassenbeheer	☒	Google Classroom
Onderwijsvoorbereiding	Opleidingsontwikkeling	☒	Google Docs/ Forms/ Drive
	Materiaalontwikkeling	☒	Google Docs/ /Slides /Drive
	Planning en roostering	☒	Google Docs
Onderwijsuitvoering	Lesuitvoering	☒	Google Presentaties/ Drive
	(Toegang tot) aanbod leermateriaal	☒	Google Classroom/ Docs/ Forms
	Toetsafname	☐	
Onderwijsevaluatie*	Beoordeling	☒	Google Docs
	Resultatenregistratie	☐	
	Terugkoppeling feedback	☒	Google Docs
Passend onderwijs *	Voortgang- en resultaatweergave	☐	
Ict-ondersteuning	Authenticatie en autorisatie	☐	
	Beheer identiteiten	☐	
	Ict-servicemanagement (device management)	☐	
Informatiebeveiliging en	Realisatie beveiligingsmaatregelen	☐	

privacy	(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:			
	...	☐	
	...	☐	

Persoonsgegevens in Google Workspace for Education.		
Betrokkene(n) (leerling, medewerkers, ouders, andere betrokkene)	Verwerkte persoonsgegevens	Motivatie
Leerling, medewerker	Voornaam	Deze gegevens zijn nodig voor het aanmaken van een account in Google Workspace for Education.
	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 (<i>Customer data</i>) in bestanden	
	Andere persoonsgegevens, namelijk:	

1.2 Beoordeling rechtmatigheid van gegevensverwerking

Vaststellen per functie of er voldaan wordt aan rechtmatigheid, d.m.v. benoeming van de grondslag en een beoordeling of er wordt voldaan aan dataminimalisatie en transparantie.

Hoofdbedrijfsfunctie	Beoordeling rechtmatigheid	
Samenwerken en communiceren medewerkers	Grondslag	Uitvoeren van een overeenkomst (i.c. de arbeidsovereenkomst)
	Dataminimalisatie	Ja/Nee Toelichting: gedeeltelijk aan voldaan.
	Transparantie	Ja/Nee

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

HOOFDBEDRIJFSFUNCTIE NIET VAN TOEPASSING		
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

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: gedeeltelijk aan voldaan.
	Transparantie	Ja/Nee

Hoofdbedrijfsfunctie	Beoordeling rechtmatigheid	
Onderwijs-ondersteuning: instroom, doorstroom, uitstroom*	Grondslag	Wettelijke verplichting (artikel 40b WPO, artikel 27b WVO, artikel 42a WEC)
	Dataminimalisatie	Ja/Nee Toelichting: gedeeltelijk aan voldaan.
	Transparantie	Ja/Nee

Hoofdbedrijfsfunctie	Beoordeling rechtmatigheid	
Onderwijs- voorbereiding	Grondslag	Uitvoeren van publieke taak (artikel 8 WPO, artikel 2 WVO, artikel 9 WEC)
	Dataminimalisatie	Ja/Nee Toelichting: gedeeltelijk aan voldaan.
	Transparantie	Ja/Nee

HOOFDBEDRIJFSFUNCTIE NIET VAN TOEPASSING		
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

HOOFDBEDRIJFSFUNCTIE NIET VAN TOEPASSING		
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

HOOFDBEDRIJFSFUNCTIE NIET VAN TOEPASSING		
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

HOOFDBEDRIJFSFUNCTIE NIET VAN TOEPASSING		
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

1.3 Maatregelen

Nog te treffen maatregelen om te voldoen aan de vereisten van rechtmatigheid (grondslag, dataminimalisatie en transparantie)	Termijn waarbinnen maatregel wordt getroffen
Dataminimalisatie: Het advies van SIVON is om zo min mogelijk gebruik te maken van echte namen van leerlingen in het emailadres. Kinderen overzien namelijk minder de gevolgen van het digitale spoor dat ze achterlaten online. Deze maatregel zorgt ervoor dat de privacy van leerlingen beter is beschermd, omdat dan uit het e-mailadres zelf geen persoon is af te leiden. Het is ook onduidelijk wat Google met deze gegevens doet. Het advies is om indien mogelijk gebruik te maken van pseudonimisering, dus gebruik van leerlingnummers in het e-mailadres, in plaats van namen. Zoals leerling123@cnbswegwijzer.nl in plaats van jandevries@cnbswegwijzer.nl. In de praktijk is gebleken dat het volledig doorvoeren van deze maatregel soms vergaande gevolgen heeft voor de gebruikers, omdat de herkenbaarheid van het emailadres hieronder leidt. De Rolfgroep heeft aangegeven dat er anonieme emailadressen aangemaakt kunnen worden met ZuluConnect, om zo 'AVG-proof' te blijven.	Advies: Aanpassen nieuwe (en waar mogelijk bestaande) emailadressen leerlingen. Voor docenten is dit nog) niet nodig. Deze optie is er bij de Rolfgroep, maar dient door de onderwijsinstelling te worden aangevraagd.
Transparantie: Momenteel is nog niet op duidelijke wijze gecommuniceerd aan betrokkenen (leerlingen en medewerkers) welke persoonsgegevens er door CNBS de Wegwijzer worden verwerkt in Google Workspace for Education. Door middel van een update van de privacyverklaring of IBP-beleid, kan hier invulling aan worden gegeven.	Advies: Updaten privacyverklaring in tweede/derde kwartaal 2022.

2 Risicoanalyse

2.1 Centraal vastgestelde risico's

In onderstaande tabel staat een overzicht van de door Google doorgevoerde maatregelen n.a.v. de centrale DPIA. Zie bijlage 2 voor een volledig overzicht.

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. <i>to provide, maintain and improve the Services and Technical Support Services (TSS) subscribed to by Customer;</i> 2. <i>to identify, address and fix security threats, risks, bugs and other anomalies</i> 3. <i>to develop, deliver and install updates to the Services subscribed to by Customer (including new functionality related to the Services subscribed to by Customer).</i>
		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 <i>gagging orders</i> 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 <i>gagging orders</i> 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 for Education 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 <u>31 December 2022</u>. Google will provide an inspection tool for admins to inspect the collected telemetry data and data generated on Google's cloud servers by <u>31 December 2022</u>. 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 <u>1 September 2021</u>. Google will make all relevant legal information about the Google Workspace for Education account permanently available in an end user notice by <u>31 December 2021</u>.
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 <i>Spelling and Grammar</i> 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.

Op basis van de bovenstaande tabel en de overige beschikbare documentatie zoals hieronder genoemd en in bijlagen is toegevoegd, wordt vastgelegd voor CNBS de Wegwijzer 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 CNBS de Wegwijzer weg te nemen?	Ja/Nee
Deze beoordeling is gebaseerd op de volgende documenten (zie bijlagen 1-5):	
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 CNBS de Wegwijzer d.d. 14-6-2022	
Raadpleging betrokkenen ((G)MR	

Indien het antwoord op bovenstaande vraag 'Nee' is, is de conclusie voor CNBS de Wegwijzer dat er geen gebruik gemaakt kan worden van Google Workspace for Education.

Hieronder staat aangegeven welke technische maatregelen CNBS de Wegwijzer (nog) niet heeft doorgevoerd, wat de planning is voor het alsnog nemen van de maatregel of de reden waarom is besloten om de maatregel niet door te voeren. Tot slot staat beschreven welke restructies het (nog) niet doorvoeren van de maatregel oplevert.

Zijn de maatregelen zoals beschreven in de <i>Handleiding technische maatregelen</i> , die op CNBS de Wegwijzer van toepassing zijn, doorgevoerd?					Ja/Nee*
*Indien het antwoord 'Nee' is vul dan onderstaande tabel verder in.					
MAATREGELN BETREFFENDE GEBRUIKERSACCOUNTS:					
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 restructie met risicoclassificatie (laag, midden, hoog)	
Gebruikersprofiel: geen gebruik maken van echte namen van leerlingen en leraren in de gebruikersnaam van Google Workspace for Education.	Nee.	Maatregel is niet doorgevoerd.	Zoals in paragraaf 1.3 besproken, is de impact van deze maatregel hoog. Er wordt gekeken wat haalbaar en of er een passende oplossing komt vanuit SIVON.	Laag	
Geografische locatie dataopslag aanpassen naar Europa.	Nee.	Maatregel is niet doorgevoerd.	Deze optie is alleen beschikbaar in bepaalde (duurdere) abonnementsvormen van Google Workspace for	Midden	

			Education.	
Aanvullende Google diensten uitschakelen	Ja.	Maatregel wordt z.s.m. doorgevoerd.	Youtube embedding wordt aanbevolen door SIVON, dit heeft niet het gewenste resultaat in de praktijk. Daarom is besloten dit voor zowel leerlingen als docenten uit te schakelen.	Laag

MAATREGELEN BETREFFENDE DATAMINIMALISATIE IN PRODUCTEN EN FUNCTIONALITEITEN:				
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)
Inloggen op de browser uitschakelen.	Nee.	Maatregel is niet doorgevoerd.	Het inloggen op de Chrome-browser zorgt er voor dat er functies zijn die goed functioneren. Als de Rolfgroep deze uitschakelt heeft dit een grote impact op de gebruikerservaring.	Midden.
Cookies van derden uitschakelen.	Nee.	Maatregel is deels doorgevoerd.	In de praktijk bleek deze maatregel niet te werken, sommige applicaties worden onbruikbaar. Er is gekozen om de maatregel door te voeren en te kijken of er voor bepaalde websites gekozen moet worden voor 'whitelisten', voor deze websites zijn de cookies dus wel toegestaan zodat ze blijven werken.	Laag.

2.2 Organisatie-specifieke risico's

Naast centraal vastgestelde risico's, is het van belang om organisatie-specifieke risico's vast te leggen. De ene onderwijsinstelling gebruikt Google Workspace for Education 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. Daarom is het van belang om te beschrijven wat de mogelijke risico's binnen de MAPGOOD-methode (Mens, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving, Diensten) zijn. Bij ieder element binnen deze methode spelen bepaalde risico's, sommige risico's liggen meer voor de hand dan andere. Hieronder is aangegeven en geclassificeerd hoe groot de gevonden risico's zijn, d.m.v. onderstaande tabel. Zie bijlage 5 voor een korte analyse die is opgesteld naar aanleiding van een vragenlijst die is beantwoord door de schooldirecteuren van CNBS de Wegwijzer.

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)

Mens

- onkunde, slordigheid
- niet werken volgens voorschriften
- fraude, sabotage

Kans: 1

Impact: 2

Risico (Kans x Impact): Laag (score: 2)

Apparatuur/programmatuur

- verouderd, onjuist functioneren
- stroomuitval

Kans: 1

Impact: 1

Risico (Kans x Impact): Laag (score: 1)

Gegevens

- ontoegankelijk
- toegankelijk voor onbevoegden
- verloren gaan

Kans: 1

Impact: 2

Risico (Kans x Impact): Laag (score: 2)

Organisatie

- onduidelijke taken, bevoegdheden
- ontbrekende gedragscodes

Kans: 1

Impact: 2

Risico (Kans x Impact): Laag (score: 2)

Omgeving

- onvoldoende beveiligde ruimtes
- natuurgeweld

Kans: 1

Impact: 1

Risico (Kans x Impact): Laag (score: 1)

Diensten

- geen goede leveranciersafspraken
- leverancier gaat failliet

Kans: 1

Impact: 2

Risico (Kans x Impact): Laag (score: 2)

In onderstaande tabel staat beschreven welke organisatie-specifieke risico's binnen CNBS de Wegwijzer zijn vastgesteld, inclusief de mitigerende maatregelen en de classificatie van het restrisico.

Beschrijving organisatie-specifiek risico	Risico score	Mitigerende maatregel(en), voorgesteld door de FG.	Binnen welke termijn is de maatregel uitgevoerd?	Classificatie risico na uitvoering maatregel (=restrisico)
Mens	2	Bewustwording d.m.v. een AVG-awareness training. Evt. 2FA doorvoeren bij het inloggen in overleg met de Rolfgroep.	Eind 2022	Laag
Apparatuur/ programmatuur	1	Structureel bijhouden van updates, in beheer van de Rolgroep.	Wordt continue en waar nodig uitgevoerd.	Laag
Gegevens	2	Bijv. d.m.v. AVG-awareness training.	Eind 2022.	Laag
Organisatie	2	Updaten + bijhouden Informatiebeveiliging en privacybeleid.	Eind 2022 / begin 2023.	Laag
Omgeving	1	In kaart brengen welke toegangen er zijn tot de schoolgebouwen en deze afsluiten indien gewenst.	Medio 2023.	Laag
Diensten	2	Updaten/actualiseren	Eind 2022 / begin	Laag

		verwerkingsregister voor het bijhouden van de verwerkingsovereenkomsten met verwerkers.	2023.	
--	--	--	-------	--

3 Conclusie onderwijsinstelling

Wanneer er geen, lage of gemiddelde restrisico's zijn vastgesteld dan maakt het bestuur van CNBS de Wegwijzer 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 een (G)MR. 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.

3.1 Advies Functionaris Gegevensbescherming

Advies Functionaris Gegevensbescherming van CNBS de Wegwijzer ten aanzien van de resultaten van onderhavige DPIA.

3.1.1 Waarnemingen

De door Google getroffen mitigerende maatregelen zoals vermeld in paragraaf 2.1 van deze DPIA, zijn door CNBS de Wegwijzer als voldoende bevonden. Deze beoordeling is gebaseerd op de maatregelen die Google heeft getroffen in respons op de centraal vastgestelde risico's. Door CNBS de Wegwijzer zijn de volgende technische maatregelen, zoals aanbevolen door Kennisnet/SIVON/SURF, in Google Workspace for Education (nog) niet doorgevoerd:

- Aanpassen/pseudonimiseren e-mailadressen.
- Geografische locatie dataopslag aanpassen naar Europa.
- Gebruikers niet laten inloggen op de Chromebrowser.

De reden hiervoor is de praktische onhaalbaarheid van deze maatregelen en de negatieve gevolgen hiervan voor gebruikers. Er is gezocht naar een werkbare situatie voor de gebruikers, die wat betreft privacyrisico's zo veilig mogelijk is ingericht. Een middenweg dus, die in de praktijk werkbaar is. De periode waarbinnen is afgesproken en vastgelegd om deze maatregelen te zullen mitigeren verschilt, in sommige gevallen is er geen termijn te geven omdat er geen goed alternatief of passende oplossing is te vinden op dit moment. Uit de gegevensverwerkingsanalyse en de beoordeling van de rechtmatigheid hiervan, zijn alleen lage restrisico's gebleken. Indien er sprake is van hoge restrisico's dan dient hiervan een melding te worden gedaan bij de Autoriteit Persoonsgegevens, dit is voor CNBS de Wegwijzer dus niet van toepassing.

3.1.2 Advies

Mijn advies is, gezien de voorgenomen én reeds doorgevoerde maatregelen en de daarbij horende lage restrisico's, dat voldoende aannemelijk is gemaakt dat de privacyrisico's die geconstateerd zijn in deze school-specifieke DPIA, voldoende zijn gemitigeerd en gering zijn ten aanzien van betrokkenen. Uit deze DPIA volgt dat er lage en middelmatige restrisico's zijn, na het toepassen van de voorhanden zijnde maatregelen. Het doorvoeren van de maatregelen, genoemd in paragraaf 1.3 en 2.2, is daarbij van belang en wordt ten eerste geadviseerd.

Dit alles in acht genomen is mijn advies dat CNBS de Wegwijzer gebruik kan blijven maken van Google Workspace for Education met de huidige toegepaste maatregelen. Mocht vanuit Kennisnet/SIVON/SURF en/of SLM Rijk nieuwe berichtgeving volgen waaruit blijkt dat er opnieuw hoge privacyrisico's zijn bij het gebruik van Google Workspace for Education, dan is mijn dringende advies om wederom kritisch te kijken naar het gebruik

van Google Workspace for Education. In zo'n situatie dient ook de FG opnieuw om een advies gevraagd te worden, teneinde gebruik te kunnen blijven maken van Google Workspace for Education. Tevens is mijn advies om één jaar na dato deze onderwijs-specifieke DPIA t.a.v. Google Workspace for Education te heroverwegen, nu er in één jaar tijd veel kan veranderen in het gebruik van softwareprogramma's zoals Google Workspace for Education.

Naam: mr. Angelique Engels

Handtekening:

Datum: 14-6-2022



3.2 Raadpleging betrokkenen

Hier dient te worden vermeld of en op welke wijze betrokkenen, zoals (G)MR zijn geraadpleegd bij deze DPIA. Indien dit niet is gebeurd, dient te worden beschreven waarom niet. Indien dit wel is gebeurd, dient hieronder de input van deze betrokkenen kort te worden toegelicht.

Input betrokkenen:

3.3 Herziening DPIA

De Autoriteit Persoonsgegevens raadt aan om DPIA's periodiek te herzien, bijvoorbeeld iedere drie jaar óf wanneer er grote wijzigingen plaats hebben gevonden in het gebruik van de software/systemen. Voor onderhavige DPIA wordt door de FG in het eerste kwartaal van 2023 gekeken of het raadzaam is om opnieuw een DPIA uit te voeren. Daarbij zal er worden geïnterviewd of het gebruik van Google Workspace for Education voor CNBS de Wegwijzer is veranderd of niet.

4 Verklaring schoolbestuur

De verwerkingsverantwoordelijke van CNBS de Wegwijzer, 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 één jaar te laten te heroverwegen door de FG en na drie jaren te 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.

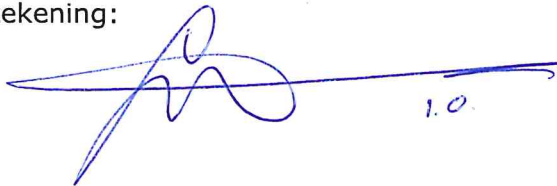
Naam onderwijsinstelling: CNBS De Wegwijzer 91079/05TF

Naam bestuurder(s): Lidy Tuin (directeur)

Plaats: Schuinesloot

Datum: 12 juli 2022

Ondertekening:



Gezien/afgehoord MR :


Jacobien Voorstok

Datum 12 juli 2022
Schuinesloot

5 Bijlagen

Bijlage 1 – Google Workspace for Education overeenkomst CNBS de Wegwijzer

Bijlage 2 – Centrale DPIA G Suite for Education d.d. 12 maart 2021

Bijlage 3 – Update SIVON/SURF omtrent Google Workspace for Education DPIA

Bijlage 4 – Kennisnet Handleiding Technische Maatregelen

Bijlage 5 – Instellingen Google Workspace De Rolfgroep.