

Gegevensbeschermingseffectbeoordeling (GEB)

Gebruik Google Workspace for Education (GWfE) door [Verwerkingsverantwoordelijke naam onderwijsinstelling(en)]

HANDLEIDING: Dit document is door de werkgroep gegevensbescherming in onderwijs opgesteld als een white label GEB voor onderwijsinstellingen die gebruik (zullen) maken van Google Workspace for Education (GWfE). Doorheen dit document zijn bepaalde tekstonderdelen **geel** gemarkeerd en tussen vierkante haken ([]) geplaatst. Deze tekstonderdelen dienen aangepast/aangevuld of geschrapt te worden door de onderwijsinstelling bij het invullen van deze GEB.

Dit document is gebaseerd op een model dat werd opgesteld door de [Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens](#) en is afgeleid van het model van het d.pia.lab van de VUB: Brussel, 2020., licentie: CC BY SA 4.0. https://researchportal.vub.be/files/53602836/dpialab_pb2020_1_final.pdf Zie ook www.dpialab.org dpialab@vub.ac.be

Inhoudstafel

1.	GEB GOOGLE WORKSPACE FOR EDUCATION	4
2.	Algemene omschrijving van de verwerking.....	5
3.	Projectstructuur	6
3.1	Deelnemers aan GEB	6
3.2	Projectwerking bij het opzetten van GEB	6
3.3	Middelen voor het uitvoeren van de GEB.....	6
3.4	(Her)evaluatie van GEB tijdens de verwerking	7
4.	Bronnen voor het opstellen van de GEB	7
4.1	Wet- en regelgeving.....	7
4.2	Aanbevelingen van EDPB/EDPS	7
4.3	Aanbevelingen en standpunten van toezichhouders	7
4.4	Aanbevelingen en standpunten van rechtbanken	8
4.5	Andere aanbevelingen.....	8
5.	Systematische beschrijving (verplicht)	9
5.1	Het toepassingsgebied van de GEB.....	9
5.2	Systematische beschrijving	11
5.3	Context van de verwerkingsactiviteit	16
5.4	Beschrijving van de betrokkenen en andere actoren	17
6.	Noodzakelijkheid en evenredigheid	20
6.1	De rechtmatigheid van de verwerking	20
6.2	De basisbeginselen van de verwerking.....	20
6.2.1	Behoorlijkheid en transparantie	20
6.2.2	Doelbinding	21
6.2.3	Minimale gegevensverwerking	21
6.2.4	Juistheid en nauwkeurigheid	22
6.2.5	Opslagbeperking	22
6.2.6	Gegevensbeveiliging.....	23
6.3	Noodzakelijkheid en evenredigheid	24
6.3.1	Noodzaak.....	Fout! Bladwijzer niet gedefinieerd.
6.3.2	Evenredigheid.....	Fout! Bladwijzer niet gedefinieerd.
7.	Methode voor beoordeling risico's op rechten en vrijheden van betrokkenen	27
7.1	Aanvaardbaarheidscriteria van negatieve effecten.....	27
7.2	Risicoanalyse, -evaluatie en opvolging	27
7.2.1	Bepalen van de impact van een risico voor betrokkene	27

7.2.2	Bepalen van de waarschijnlijkheid van een risico voor betrokkene	28
7.2.3	Bepalen van de risicomatrix.....	29
8.	Beoordeling risico's op rechten en vrijheden van betrokkenen	30
9.	Beoogde maatregelen om risico's aan te pakken.....	31
10.	Mening betrokkenen/vertegenwoordigers over de verwerking.....	32
11.	Adviezen betreffende de GEB.....	33
11.1	Advies functionaris voor gegevensbescherming	33
11.2	Voorafgaande raadpleging bij de toezichthouder (verplicht bij hoog restrisico).....	33
11.3	Overzicht van de acties die de verwerkingsverantwoordelijke neemt naar aanleiding van het advies van de functionaris en de raadpleging van de toezichthouder	33
12.	Besluit van de verwerkingsverantwoordelijke	34

1. GEB GOOGLE WORKSPACE FOR EDUCATION

Naam/referentie van het initiatief:	GWfE Fundamentals
Naam, contactinformatie en andere identificatiegegevens van:	
Verwerkingsverantwoordelijke(n) en hun vertegenwoordigers:	[Naam Verwerkingsverantwoordelijke van onderwijsinstelling(en)] Hierna verwerkingsverantwoordelijke genoemd
Verantwoordelijke(n) voor het project (business owner):	
Functionaris(sen) voor gegevensbescherming (DPO)¹:	
Versie van GEB:	GWfE – Fundamentals
Referentie naar pre-GEB:	N/A
Classificatie:	☐ Publiek ☐ Vertrouwelijk ☐ Informatieklasse [1/2/3/4/5] ...

¹ Alle Vlaamse bestuursinstanties moeten een functionaris aangesteld hebben en hun verwerkers ook.

² De Vlaamse Toezichtcommissie voor de Vlaamse bestuursinstanties.

2. Algemene omschrijving van de verwerking

Onderwijsinstellingen maken gebruik van diverse digitale hulpmiddelen om zowel hun primaire als secundaire processen te ondersteunen en kwalitatief onderwijs aan te bieden aan leerlingen. Primaire processen omvatten de kernactiviteiten van onderwijs, zoals lesgeven, leren en begeleiding van leerlingen. Secundaire processen omvatten ondersteunende taken, zoals administratie, personeelsbeheer en communicatie.

Een van de digitale hulpmiddelen die de verwerkingsverantwoordelijke inzet of overweegt in te zetten, is Google Workspace for Education (GWfE). Dit cloudgebaseerde platform biedt een uitgebreid pakket tools, specifiek ontworpen om het digitale leerproces te faciliteren, en om samenwerking en communicatie binnen de onderwijscontext te bevorderen.

Google Workspace for Education wordt aangeboden in verschillende versies, zowel gratis (GWfE Fundamentals) als betalend (GWfE Standard, GWfE Plus). Binnen het platform wordt telkens een onderscheid gemaakt tussen:

- **Kernservices:** Deze vormen de basis van Google Workspace for Education en zijn specifiek ontwikkeld voor educatief gebruik. Voorbeelden zijn Google Classroom, Gmail, Google Drive, Google Documenten, Google Agenda en Google Meet.
- **Aanvullende services:** Deze diensten, zoals onder andere YouTube, Google Maps en Blogger, zijn in eerste instantie ontwikkeld voor consumenten maar kunnen optioneel in een educatieve context worden gebruikt.

Deze gegevensbeschermingseffectbeoordeling (GEB) richt zich op het gebruik van alle kernservices van Google Workspace for Education Fundamentals, de meest gebruikte versie binnen Vlaamse onderwijsinstellingen. Het doel van deze GEB is om inzicht te krijgen in de verschillende verwerkingen van persoonsgegevens, om de risico's te bepalen die aan de verwerkingen verbonden zijn en om de naleving van de AVG te waarborgen. Door deze GEB uit te voeren, willen we ervoor zorgen dat de verwerking van persoonsgegevens binnen Google Workspace for Education Fundamentals op een veilige en verantwoorde manier gebeurt, waarbij de privacy van alle betrokkenen wordt beschermd.

Aanvullende services vallen buiten de scope van deze GEB.

Deze GEB wordt uitgevoerd op initiatief van de expertenwerkgroep in het kader van haar opdracht om de gegevensbescherming binnen het Vlaamse onderwijsveld te versterken. De expertenwerkgroep erkent dat een GEB in principe voorafgaand aan de implementatie van een softwareplatform moet worden uitgevoerd (privacy by design). Omdat Google Workspace for Education reeds breed in gebruik is bij Vlaamse onderwijsinstellingen, richt deze GEB zich op de bestaande verwerkingen en de persoonsgegevens die hierbij worden verwerkt. Deze GEB onderzoekt de risico's die aanwezig zijn bij het gebruik van Google Workspace for Education en welke maatregelen kunnen genomen worden om de bescherming van de persoonsgegevens te kunnen waarborgen.

Als onderdeel van deze GEB wordt een technische handleiding toegevoegd waarin de aanbevolen privacy-instellingen van Google Workspace for Education worden beschreven (bijlage 3).

3. Projectstructuur

3.1 Deelnemers aan GEB

Deze analyse werd uitgevoerd in opdracht van de expertenwerkgroep gegevensbescherming in onderwijs¹ en is het resultaat van een samenwerking tussen AVG-experten van het agentschap Digitaal Vlaanderen en AVG-experten, beheerders en gebruikers van Google Workspace for Education uit de onderwijsnetten van het Deeltijds Kunstonderwijs, LIGO, Centra voor Basiseducatie, het Gemeenschapsonderwijs (GO!), het Gemeentelijk Onderwijs en het Katholiek Onderwijs Vlaanderen.

Volgende profielen namen deel aan de GEB:

- (Pedagogisch) ICT-coördinatoren
- Functionarissen gegevensbescherming (DPO)
- Beleidsmedewerkers

Als er vragen zijn in verband met deze GEB, kan de onderwijsinstelling contact opnemen met de lokale functionaris voor gegevensbescherming, ook wel Data Protection Officer (DPO) genoemd. Onderwijsinstellingen kunnen ook de DPO van de scholengemeenschap of het onderwijsnet contacteren.

De analyse voor de verwerkingsverantwoordelijke werd uitgevoerd door

3.2 Projectwerking bij het opzetten van GEB

De werkgroep Google Workspace for Education heeft de GEB uitgevoerd door tijdens (twee)wekelijkse vergaderingen de verwerkingen te analyseren.

De verwerkingsverantwoordelijke kan hier aangeven op welke manier de analyse van de GEB binnen zijn onderwijsinstelling gebeurt.

Voorbeeld: [VERWERKINGSVERANTWOORDELIJKE VAN NAAM ONDERWIJSINSTELLING(EN)] maakt gebruik van Google Workspace for Education waardoor het uitvoeren een GEB noodzakelijk is. De GEB wordt besproken tijdens een wekelijkse ICT-werkgroep. Zodra de GEB gefinaliseerd is, wordt deze ter advies voorgelegd aan de DPO.....

3.3 Middelen voor het uitvoeren van de GEB

Voor de GEB zijn voldoende middelen voorzien om te garanderen dat de uitvoering objectief en correct kan plaatsvinden. Om concreet de diverse aspecten te benoemen die onderbouwen dat voldoende middelen zijn ingezet:

- Expertengroep gegevensbescherming in onderwijs: Deze expertengroep richt zich in eerste instantie op de coördinatie van de generiek uit te voeren gegevensbeschermingseffectbeoordelingen op EdTech-software die in onderwijs gebruikt wordt en het aanpakken van eventuele nieuwe privacyrisico's en dit in een continu proces.

¹ [Privacy in het onderwijs \(privacyinonderwijs.be\)](https://www.privacyinonderwijs.be)

- Tijdsbesteding actoren: Voor de uitvoering van de GEB is input verzameld vanuit het onderwijsveld. Personen uit onderwijsinstellingen en de expertenwerkgroep onderwijs zijn hiervoor vrijgemaakt. Daarnaast werken de koepels en netwerkverenigingen samen met het Departement Onderwijs en Vorming en het agentschap Digitaal Vlaanderen om zowel inhoudelijke als technische input aan te leveren.

3.4 (Her)evaluatie van GEB tijdens de verwerking

Het is belangrijk om een GEB samen te laten evolueren met de verwerkingsactiviteiten die in deze GEB worden beoordeeld.

Indien nodig, zal de verwerkingsverantwoordelijke deze GEB aanpassen of actualiseren. Dit kan nodig zijn in het kader van wijzigingen van het gegevensverwerkingsproces, nieuwe ontwikkelingen in de gebruikte technologie, of uitspraken en beslissingen van de bevoegde rechtbanken en toezichthoudende autoriteiten.

In elk geval wordt deze GEB minstens tweejaarlijks geëvalueerd.

4. Bronnen voor het opstellen van de GEB

Hieronder worden de bronnen opgelijst die worden gebruikt bij het opstellen van de GEB.

4.1 Wet- en regelgeving

- [Verordening \(EU\) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG \("AVG"\)](#);
- [Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens \("Kaderwet"\)](#);
- [Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer \("eGOV-decreet"\)](#);
- [Vlaams Bestuursdecreet van 7 december 2018 \("Bestuursdecreet"\)](#);
- [Decreet basisonderwijs \(vlaanderen.be\)](#)
- [Gecodificeerd Decreet betreffende het secundair onderwijs \[citeeropschrift: "Codex Secundair Onderwijs"\] \(vlaanderen.be\)](#)
- [Decreet betreffende het deeltijds kunstonderwijs \(vlaanderen.be\)](#)
- [Decreet betreffende de rechtspositie van de personeelsleden in de basiseducatie \(citeeropschrift: decreet Rechtspositie Basiseducatie\) \(vlaanderen.be\)](#)
- [Decreet over leersteun \(vlaanderen.be\)](#)
- Digisprong gewoon en buitengewoon kleuter-, lager en secundair onderwijs: [omzendbrief NO/2021/03 van 31/05/2021 \(vlaanderen.be\)](#)

4.2 Aanbevelingen van EDPB/EDPS

- EDPB Use of cloud-based services by the public sector: [edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf \(europa.eu\)](#)
- EDPB Adequaatheidsbesluit: [edpb_informationnoteadequacydecisionus_en.pdf](#)

4.3 Aanbevelingen en standpunten van toezichthouders

- [Advies AP Google-producten in het onderwijs | Autoriteit Persoonsgegevens](#)
- Recommendations on Digital rights of children: <https://www.cnil.fr/en/digital-rights-children>
- Age appropriate design: a code of practice: <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>
- The DPC Fundamentals for a Child-Oriented Approach to Data Processing: <https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing>
- Deense toezichthouders: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/datatilsynet-giver-paabud-i-chromebook-sag>
- GBA: brochure [keuze verwerkers voor onderwijsinstellingen](#)
- VTC: [Richtlijnen](#) van de Vlaamse Toezichtcommissie bij het gebruik van digitale middelen in het onderwijs zoals leerlingen, cursisten- en personeelsadministratie, leerlingvolgsystemen, pakketten voor financieel beheer, educatief lesmateriaal en elektronische leeromgevingen ...
- VTC: Cloudadvies [VTC A 2020 05 advies gous2z.pdf \(vlaanderen.be\)](#) en [VTC A 2022 02 voor publicatie def G.pdf \(vlaanderen.be\)](#)
- Standpunt van Vlaamse Toezichtcommissie (VTC) i.v.m. gebruik Google for Education door basis- en secundair onderwijs: [VTC O 2023 01 brief VTC lckjxs.pdf \(vlaanderen.be\)](#)
- Brief van Vlaamse Toezichtcommissie aan de leden van de expertenwerkgroep i.v.m. Google Workspace for Education: [VTC O 2023 01 brief VTC k7dx05.pdf \(vlaanderen.be\)](#)

4.4 Aanbevelingen en standpunten van rechtbanken

Niet van toepassing

4.5 Andere aanbevelingen

- GEB Nederland (SUFR/SIVON): [Alles over de DPIA's op Google Workspace & ChromeOS - SIVON](#)
- GEB Noorwegen: [New national DPIA for the use of Google Workspace for Education in Norwegian Schools - Hjem](#)

5. Systematische beschrijving (verplicht)

5.1 Het toepassingsgebied van de GEB

In deze gegevensbeschermingseffectbeoordeling (GEB) wordt een overzicht gegeven van de belangrijkste verwerkingen die plaatsvinden binnen de primaire en secundaire processen van onderwijsinstellingen. Deze processen zijn geanalyseerd met specifieke aandacht voor de rol van verschillende betrokkenen, zoals leerlingen, leerkrachten, andere personeelsleden binnen een onderwijsinstelling en ouders.

De focus ligt op de verwerking van persoonsgegevens die noodzakelijk zijn om deze processen te ondersteunen. Hierbij wordt rekening gehouden met de unieke behoeften en verantwoordelijkheden van onderwijsinstellingen, waaronder:

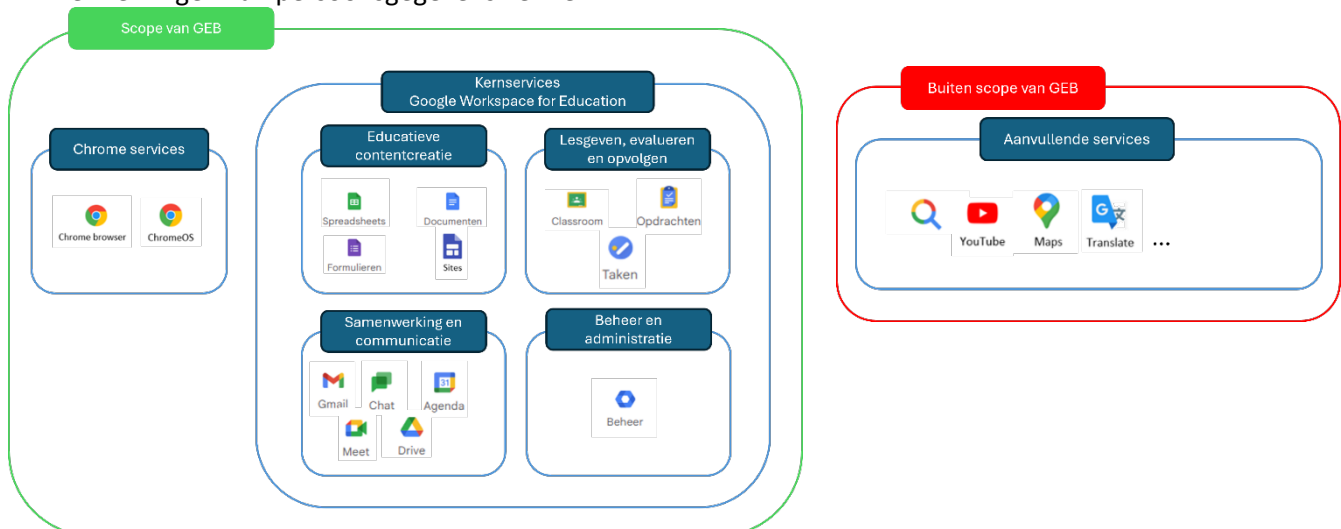
- het bieden van kwalitatief onderwijs aan leerlingen (primaire processen);
- het beheren van administratieve, organisatorische en ondersteunende taken (secundaire processen).

Daarnaast wordt onderzocht welke kernservices van Google Workspace for Education (GWfE) kunnen worden ingezet om deze processen te faciliteren. Deze tools bieden onderwijsinstellingen de mogelijkheid om efficiënt samen te werken, te communiceren en onderwijsactiviteiten te organiseren binnen een veilige digitale omgeving.

Door deze aspecten in kaart te brengen, beoogt deze GEB een heldere basis te bieden voor het veilig en verantwoord gebruik van Google Workspace for Education binnen de onderwijsinstellingen van de verwerkingsverantwoordelijke, in lijn met de geldende privacywetgeving en de behoeften van de betrokkenen.

Kernservices en aanvullende services

Binnen deze GEB worden alle kernservices van Google Workspace for Education Fundamentals (de gratis versie van GWfE) meegenomen, omdat ze onder dezelfde contractuele voorwaarden vallen en vergelijkbare verwerkingen van persoonsgegevens kennen.



Binnen het kader van deze GEB worden de kernservices van Google Workspace for Education gegroepeerd in vier hoofdcategorieën. Deze kernservices ondersteunen op een geïntegreerde manier het onderwijsproces en worden als volgt ingedeeld:

1. Educatieve contentcreatie

Deze categorie omvat tools die leerlingen en onderwijspersoneel in staat stellen om educatieve inhoud te creëren, bewerken en delen. Denk hierbij aan tekstverwerking, presentaties, spreadsheets en het bouwen van eenvoudige websites. Voorbeelden van toepassingen zijn Documenten, Spreadsheets, Presentaties, Formulieren en Sites.

2. Lesgeven, evalueren en opvolgen

Deze tools bieden ondersteuning bij het plannen, geven en opvolgen van lessen en opdrachten. Ze stellen leerkrachten in staat om opdrachten uit te reiken, evaluaties uit te voeren en feedback te geven. Belangrijke toepassingen zijn onder andere Classroom, Opdrachten en Tasks.

3. Samenwerking en communicatie

Deze diensten bevorderen samenwerking en communicatie tussen leerlingen, leerkrachten en andere betrokkenen. Ze omvatten onder meer e-mail, chat, agenda, videomeetings en bestandsdeling. Voorbeelden zijn Gmail, Chat, Agenda, Meet en Drive.

4. Beheer en administratie

Voor het beheren van gebruikers, instellingen en groepen binnen de onderwijsinstelling zijn er beheertools beschikbaar. Deze bieden controle over de digitale omgeving en zorgen voor een veilige en efficiënte werking. Tot deze groep behoren onder andere Admin Console, Groepen en Contacten.

De kernservices bevatten geen advertenties en gebruiken de informatie die ze bevatten niet voor advertentiedoeleinden.

De aanvullende services van GWfE Fundamentals² zoals bijvoorbeeld YouTube, Google Search en Google Maps worden niet geanalyseerd in deze GEB. Deze services zijn algemeen beschikbaar voor alle consumenten. Om deze aanvullende services te kunnen gebruiken, moet de onderwijsinstelling deze bewust activeren. Bovendien is het noodzakelijk om de toestemming van de ouders te hebben om aanvullende services zonder leeftijdsbeperkingen te kunnen gebruiken. Richtlijnen over het gebruik van de aanvullende services zijn terug te vinden in bijlage 2 en 3.

Chromebooks

Veel onderwijsinstellingen die gebruikmaken van Google Workspace for Education (GWfE) doen dit in combinatie met Chromebooks, waarbij ChromeOS en de Chrome-browser een belangrijke rol spelen in de digitale leeromgeving.

² [Kernservices en aanvullende services van Google Workspace for Education](#)

Voor deze specifieke producten – ChromeOS en de Chrome-browser – werd in deze GEB enkel gekeken naar de contractuele voorwaarden die Google biedt binnen het kader van educatie. Dit betreft de afspraken en voorwaarden die specifiek van toepassing zijn op het gebruik van deze producten binnen de onderwijssector. De contractuele bepalingen voor ChromeOS en de Chrome-browser zijn van belang, aangezien ze invloed hebben op de gegevensverwerking binnen de onderwijsinstellingen die deze technologieën inzetten. Deze voorwaarden zorgen ervoor dat de onderwijsinstellingen voldoen aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) en dat de verwerking van persoonsgegevens op een verantwoorde manier gebeurt.

5.2 Systematische beschrijving

Google Workspace for Education is een onderdeel van Google for Education, een bredere tak van Google die zich richt op het leveren van technologie en middelen om het onderwijs te transformeren.

Om gebruik te kunnen maken van Google Workspace for Education is een account nodig. Dit account wordt beheerd door een onderwijsinstelling, en wordt gebruikt door leerlingen en personeelsleden van de onderwijsinstelling. Het account kan worden gebruikt voor zowel kern- als aanvullende services. Beheerders beheren hoe leerlingen kern- en aanvullende services met hun Google Workspace for Education-account gebruiken. De aanvullende services vallen niet onder de voorwaarden van Google Workspace for Education.

Voor het in gebruik nemen van een account in Google Workspace for Education en het gebruik van ChromeOS en de Chrome-browser op beheerde Chromebooks, is een beperkte set van gegevens nodig van de betrokkene (leerling of personeelsleden van de onderwijsinstelling). Dit betreft de voornaam, naam, wachtwoord en school-e-mailadres. Het is hierbij niet noodzakelijk om de volledige voor- en achternaam van een betrokkene te gebruiken. Er wordt geadviseerd om in het e-mailadres geen volledige naam op te nemen³.

Wat betreft het gebruik van ChromeOS en de Chrome-browser op beheerde Chromebooks, wordt gebruikgemaakt van device- en identitymanagement binnen Google Workspace for Education. Voor deze toepassingen zijn verder geen aanvullende gegevens vereist. Het beheer van Chromebooks vereist wel een specifieke licentie, namelijk de Chrome Education Upgrade, die nodig is voor de volledige levensduur van het apparaat.

In deze gegevensbeschermingseffectbeoordeling (GEB) worden de verwerkingsactiviteiten binnen onderwijsinstellingen onderverdeeld in twee hoofdcategorieën: primaire en secundaire onderwijsprocessen. Deze indeling helpt om het doel en de context van de gegevensverwerking correct te duiden, met het oog op een transparante risicoanalyse en passende beveiligingsmaatregelen.

- **Primaire onderwijsprocessen**

Dit zijn de kernactiviteiten van de school die rechtstreeks bijdragen aan het leerproces van de leerling. Ze omvatten alle handelingen die betrekking hebben op het geven van les, het begeleiden van leeractiviteiten, het begeleiden van leerlingen en het beoordelen van leerprestaties. Verwerkingen binnen deze categorie staan in direct verband met de onderwijskundige opdracht van de instelling.

³ [google workspace edu data protection implementation guide.pdf](#)

- **Secundaire onderwijsprocessen**

Alle andere processen die het primaire onderwijsproces mogelijk maken of ondersteunen, worden als secundair beschouwd. Het gaat hierbij om administratieve, organisatorische, technische en begeleidende processen die niet rechtstreeks tot het leerproces behoren, maar die wel noodzakelijk zijn voor een goed functionerende schoolwerking. Ook communicatie met ouders, personeelsbeheer en inschrijvingen vallen onder deze categorie.

De persoonsgegevens die vermeld worden zijn persoonsgegevens die door onderwijsinstellingen in deze processen kunnen verwerkt worden, niet noodzakelijk door Google Workspace for Education.

Categorieën van persoonsgegevens die door onderwijsinstellingen kunnen verwerkt worden, zijn: **professionele contactgegevens, persoonlijke contactgegevens, identificatiegegevens, persoonlijke kenmerken, rijksregisternummer, financiële en fiscale gegevens, samenstelling gezin, algemene, fysieke kenmerken, medische of psychische gegevens en behandelingen, opleiding, ervaring en vorming, evaluaties en prestaties, en leefgewoonten.**

Ook de bijzondere categorieën van persoonsgegevens zoals vermeld in artikel 9 AVG kunnen door onderwijsinstellingen verwerkt worden. Het kan dan gaan om **persoonsgegevens waaruit ras of etnische afkomst, religieuze of levensbeschouwelijke overtuigingen blijken, gegevens over gezondheid of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid**. Deze persoonsgegevens worden enkel verwerkt met de uitdrukkelijke toestemming van de betrokkene of de ouders.

Hieronder wordt een overzicht gegeven van de verwerking van persoonsgegevens binnen de primaire en secundaire onderwijsprocessen. Dit overzicht is ook terug te vinden in bijlage 1.

Het is de bedoeling dat [VERWERKINGSVERANTWOORDELIJKE NAAM ONDERWIJSINSTELLING(EN)] in bijlage 1 in de kolom 'Verwerkte persoonsgegevens' invult welke persoonsgegevens effectief verwerkt worden. In de kolom 'Google Workspace for Education' geeft de [VERWERKINGSVERANTWOORDELIJKE NAAM ONDERWIJSINSTELLING(EN)] aan of voor dit onderwijsproces al dan niet de kernservices van Google Workspace for Education gebruikt worden.

Primaire onderwijsprocessen

Proces	Omschrijving	Verwerkte persoonsgegevens	Betrokkene
Onderwijs en lesgeven	Het lesgeven aan leerlingen en het begeleiden van leerlingen in hun leerproces.	Naam, voornaam, klas, aanwezigheid, leerprestaties, voortgang, leerondersteunende middelen	Leerling
Leerlingbegeleiding en zorg voor leerlingen	Het bieden van ondersteuning aan leerlingen op vlak van leren, sociaal-emotionele ontwikkeling, of medische noden.	Naam, voornaam, geboortedatum, sociale achtergrond, interesses, leerproblemen, evaluatieresultaten, verslagen externe begeleiding (indien van toepassing), oriënteringsadvies	Leerling

Proces	Omschrijving	Verwerkte persoonsgegevens	Betrokkene
	Het begeleiden van de leerling bij studieoriëntering en keuze van verdere studierichtingen.	medische gegevens, psychologische gegevens	
Evalueren van leerlingen	Het meten en beoordelen van de leerprestaties van de leerling, zoals toetsen en examens.	Naam, voornaam, klas, vakkenpakket, evaluatieresultaten, aanwezigheid tijdens evaluaties, speciale ondersteuningsnoden (indien van toepassing)	Leerling
Tucht en Discipline	Het behandelen van disciplinaire kwesties zoals sancties of maatregelen.	Naam, voornaam, klas, feiten betreffende het incident, eventuele getuigenverklaringen, disciplinaire voorgeschiedenis, communicatie met betrokkenen, rapportering aan externe instanties (indien van toepassing)	Leerling
Overgang naar ander onderwijs	Administratieve afhandeling wanneer een leerling van school of onderwijsniveau verandert.	Naam, voornaam, geboortedatum, adres, evaluatieresultaten, voorgaande school, attest van verworven competenties, verslagen externe begeleiding (indien van toepassing)	Leerling
Attesten en diploma's uitreiken	Het uitreiken van een officieel attest of diploma aan de leerling bij het beëindigen van een opleiding.	Naam, voornaam, geboortedatum, klas, resultaten, officieel onderwijsnummer, handtekening schooldirecteur	Leerling

Secundaire onderwijsprocessen

Proces	Omschrijving	Verwerkte persoonsgegevens	Betrokkene
Aanmelding	Het proces waarbij een leerling zich aanmeldt voor een school.	Naam, voornaam, geboortedatum, rijksregisternummer, contactgegevens van ouders/voogd, adresgegevens, voorkeursschool, relatie tot leerling (ouders/voogd), burgerlijke staat ouders/voogd	Leerling Ouder(s), voogd

Proces	Omschrijving	Verwerkte persoonsgegevens	Betrokkene
Inschrijving	Het formeel inschrijven van een leerling in een school, na de aanmelding.	Naam, voornaam, geboortedatum, rijksregisternummer, nationaliteit, contactgegevens ouders/voogd, adresgegevens, medische gegevens (indien van toepassing), schoolverleden, thuistaal ouders, keuze voor levensbeschouwelijk vak, rijksregisternummer ouders/voogd, relatie tot leerling (ouders/voogd), burgerlijke staat ouders/voogd, diploma moeder	Leerling Ouder(s), voogd
Start administratieve dossieropbouw	Het aanmaken van een leerlingendossier waarin persoonlijke en administratieve gegevens worden verzameld.	Naam, voornaam, rijksregisternummer, geboortedatum, adres, profielfoto, studiekeuze, schoolverleden, nationaliteit, taalkeuze, contactinformatie, medische gegevens (indien relevant), nood aan leerondersteuning, financiële situatie	Leerling Ouder(s), voogd
Administratief personeelsdossier	Het aanmaken van een personeelsdossier waarin persoonlijke en administratieve gegevens worden verzameld.	Naam, voornaam, geboortedatum, e-mailadres, adres, profielfoto, telefoonnummer, gsmnummer, diploma, financiële gegevens, looncategorie, stamboeknummer, rijksregisternummer	Leerkracht Ondersteunend personeel
Account aanmaken	Het aanmaken van een account om toegang te krijgen tot digitale platformen.	Naam, voornaam, e-mailadres, klas of groep, gebruikersnaam, wachtwoord	Leerling, Leerkracht Ondersteunend personeel
Schoolorganisatie	De toewijzing van de leerling aan een bepaalde klas en leerkracht.	Naam, voornaam, studiekeuze	Leerling Leerkracht
Communicatie met ouders, leerlingen, leerkrachten, onderwijspersoneel	Contact houden met ouders/voogden over de voortgang van de leerling en praktische zaken. Onderwijspersoneel houdt contact met	Contactgegevens ouders/voogd, naam en voornaam leerling, e-mailadres, klas, evaluatieresultaten, relatie tot leerling, gsmnummer	Leerling Ouder(s), voogd Leerkracht Ondersteunend personeel

Proces	Omschrijving	Verwerkte persoonsgegevens	Betrokkene
	elkaar en met leerlingen over opdrachten.		
Archiveren en bewaren van gegevens	Het bewaren van het leerlingendossier voor administratieve en wettelijke doeleinden na afstuderen of schoolverlating.	Naam, voornaam, geboortedatum, rijksregisternummer, evaluatieresultaten, attesten en diploma's	Leerling
Financieel beheer	Het financieel beheer van de school bijvoorbeeld schoolrekeningen	Naam, voornaam, adres, bankrekeningnummer	Leerling Ouders/voogd Leerkracht Ondersteunend personeel
Fiscaal beheer	Fiscale attesten	Naam, voornaam, rijksregisternummer ouders/voogd	Leerling Leerkracht
Logging en monitoring	Bijhouden van loggegevens	IP-adres, naam, voornaam, accountnaam, datum en tijdstip van aanmelding	Leerling Leerkracht Ondersteunend personeel
Sollicitatie kandidaten onderwijspersoneel	Het bijhouden van sollicitaties van mogelijk nieuwe leerkrachten of ander onderwijspersoneel	Naam, voornaam, geboortedatum, e-mailadres, adres, telefoonnummer, gsmnummer, loopbaan, diploma	Kandidaat-leerkracht of ander toekomstig personeel onderwijsinstelling
Evaluatie van personeelsleden	Evaluatie van leraren en personeelsleden	Naam, voornaam, evaluatieverslag	Leerkracht Ondersteunend personeel

Proces	Omschrijving	Verwerkte persoonsgegevens	Betrokkene
Tucht en discipline personeelsleden		Naam, voornaam, incident, getuigen (indien van toepassing), beroepsprocedure	Leerkracht Ondersteunend personeel

5.3 Context van de verwerkingsactiviteit

Digitalisering is niet meer weg te denken uit de hedendaagse maatschappij. Ook binnen het onderwijs wordt volop ingezet op digitalisering, zowel in de primaire onderwijsprocessen zoals lesgeven, als in de secundaire, ondersteunende onderwijsprocessen.

Onderwijsinstellingen maken voor hun primaire onderwijsopdrachten gebruik van diverse educatieve en pedagogische digitale hulpmiddelen. De eindtermen die leerlingen moeten bereiken, worden geformuleerd in functie van sleutelcompetenties. Eén van die sleutelcompetenties, zowel in het basisonderwijs (artikel 44, §2 van het decreet basisonderwijs) als in het secundair onderwijs (artikel 139, §2 van het Gecodificeerd Decreet betreffende het Secundair Onderwijs), is 'digitale competentie en mediawijsheid'. Leerlingen worden aangemoedigd om op een correcte en bewuste manier om te gaan met digitale hulpmiddelen en om de nodige digitale vaardigheden te ontwikkelen. Ook in de toekomstige minimumdoelen⁴ zal verder ingezet worden op het computationeel denken en de digitale zelfredzaamheid.

Educatieve softwarepakketten worden dan ook gekozen na een weloverwogen screening. De keuze hangt af van verschillende criteria, waaronder het pedagogisch project van de onderwijsinstelling, de kostprijs, het gebruiksgemak voor leerlingen, de mate van integratie met andere toepassingen en de uniformiteit in gebruikservaring (zoals een gelijkaardige look-and-feel tussen tools, wat de digitale toegankelijkheid en de overdracht van vaardigheden tussen verschillende platformen ondersteunt), en uiteraard ook de naleving van de Algemene Verordening Gegevensbescherming (AVG).

Daarnaast speelt ook het beheer en de beveiliging van het softwarepakket een belangrijke rol. Een platform dat centrale beheerfunctionaliteiten aanbiedt, laat onderwijsinstellingen toe om gebruikersrechten, toegangsniveaus en privacy-instellingen op een consistente en efficiënte manier te beheren. Dit is des te belangrijker gezien onderwijsinstellingen doorgaans over beperkte middelen en personeelscapaciteit beschikken voor ICT-beheer. Het technisch beheer wordt vaak toevertrouwd aan een ICT-coördinator, die meerdere taken combineert en nood heeft aan overzichtelijke en gebruiksvriendelijke beheertools. Een goed beheersbaar platform ondersteunt zo niet alleen de veiligheid, maar ook de werkbaarheid in de praktijk.

Ook ondersteunende onderwijsprocessen worden verder gedigitaliseerd. Om deze processen efficiënt te laten verlopen, wordt even zorgvuldig nagedacht over de juiste keuze van software.

Eén van de digitale hulpmiddelen die leerkrachten als educatieve tool gebruiken, en dat een geïntegreerd onderdeel vormt van het leer- en onderwijsproces, is Google Workspace for Education. De persoonsgegevens die via dit platform worden verzameld, worden verwerkt met het oog op communicatie, samenwerking en toegang tot leermiddelen, in lijn met het streven van de onderwijsinstelling om de digitale competenties van haar leerlingen te versterken.

⁴ [Onderwijsdoelen](#)

5.4 Beschrijving van de betrokkenen en andere actoren

Hieronder wordt een overzicht gegeven van de betrokkenen, evenals van de rollen van de verwerkingsverantwoordelijke(n) en de verwerker.

Om die rollen correct te kunnen bepalen, is het belangrijk om het onderscheid te begrijpen tussen twee soorten gegevens⁵ die Google verwerkt wanneer betrokkenen gebruikmaken van Google Workspace for Education:

- Klantgegevens: informatie die door gebruikers via de kernservices wordt verstrekt.
- Servicegegevens: informatie die door Google wordt verzameld tijdens het gebruik van die kernservices.

Klantgegevens worden verwerkt volgens de instructies van de onderwijsinstelling, die in dit geval optreedt als verwerkingsverantwoordelijke. Het gaat om gegevens die door betrokkenen worden ingediend, opgeslagen, verzonden of ontvangen via de kernservices. Voorbeelden zijn gebruikersnamen, e-mailadressen, wachtwoorden, maar ook inhoud van e-mails, documenten, en andere leermaterialen. Deze gegevens worden verwerkt tijdens het gebruik van Google Workspace for Education.

Servicegegevens daarentegen worden verzameld en verwerkt door Google zelf met het oog op het leveren, onderhouden en beveiligen van deze diensten. Het gaat hierbij om metadata zoals bijvoorbeeld gebruikersactiviteit, informatie over het gebruik van apps, browser- en apparaatgegevens, informatie uit supporttickets en locatie-informatie. Servicegegevens zijn dus geen inhoudelijke gegevens (zie klantgegevens), maar zijn vooral log- en systeemgegevens die automatisch gegenereerd worden bij het gebruik van Google Workspace for Education.

Google gebruikt deze gegevens om technische problemen op te lossen, beveiligingsmaatregelen up-to-date te houden, ondersteuning te bieden, en om aanbevelingen te formuleren ter verbetering van het gebruik van de services.

Afhankelijk van de contractuele overeenkomst die de verwerkingsverantwoordelijke met Google aangaat, neemt Google de rol op van verwerker of van verwerkingsverantwoordelijke. In onderstaand schema wordt dit verduidelijkt. Hieruit blijkt dat het gebruik van de kernservices van Google Workspace for Education enkel met een Service Data Addendum⁶ mogelijk is. Enkel op die manier is (het schoolbestuur van) de onderwijsinstelling de verwerkingsverantwoordelijke. Het is belangrijk dat de [VERWERKINGSVERANTWOORDELIJKE NAAM ONDERWIJSINSTELLING(EN)] de individuele overeenkomst met Google nagaat en de rollen en verantwoordelijkheden beoordeelt.

Dienst		Verwerkingsverantwoordelijke	Verwerker
Kernservices van Google Workspace for Education zonder Service Data Addendum	Persoonsgegevens van gebruikers (klantgegevens)	Schoolbestuur	Google

⁵ https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-your-info

⁶ [Google Workspace for Education Service Data Addendum](#)

Dienst		Verwerkingsverantwoordelijke	Verwerker
	Servicegegevens	Google ⁷	-
Kernservices van Google Workspace for Education met Service Data Addendum	Persoonsgegevens van gebruikers (klantgegevens)	Schoolbestuur	Google
	Servicegegevens	Schoolbestuur ⁸	Google

Betrokkenen

De betrokkenen zijn degenen van wie de persoonsgegevens verwerkt worden. Dit zijn leerlingen, ouders, (interim)leerkrachten, zorgcoördinatoren, ICT-coördinatoren, beheerders, secretariaat/ondersteunend personeel, directie, bestuurders ...

In punt 5.2 wordt aangeduid welke persoonsgegevens van de betrokkenen de onderwijsinstellingen in Google Workspace for Education kunnen verwerken.

Ontvangers

De derden/ontvangers zijn degenen die de verwerkte persoonsgegevens kunnen ontvangen. Dit zijn onder andere CLB, leersteuncentra, lokaal bestuur ...

Verwerkingsverantwoordelijke

Het schoolbestuur van de onderwijsinstelling(en) wordt als verwerkingsverantwoordelijke beschouwd. Dit betekent dat het schoolbestuur het doel en de middelen van de verwerking bepaalt, en zelf moet inschatten of het gebruik van de kernservices van Google Workspace for Education gepast is voor zijn of haar onderwijsinstelling(en).

Als het schoolbestuur geen Service Data Addendum afgesloten heeft, treedt Google ook op als verwerkingsverantwoordelijke voor de 'servicegegevens' binnen Google Workspace for Education. Dit betekent dat Google doel en middelen bepaalt van de verwerking van de persoonsgegevens van leerlingen, leerkrachten en anderen. Google Workspace for Education verwerkt deze gegevens om bestaande en nieuwe commerciële diensten verder te ontwikkelen.

Door het afsluiten van een Service Data Addendum mag Google slechts in beperkte gevallen de servicegegevens als verwerkingsverantwoordelijke gebruiken, namelijk voor facturatie, interne rapportages, misbruikdetectie, verwerking van supporttickets en om te voldoen aan wettelijke verplichtingen.

Google mag de servicegegevens contractueel niet gebruiken voor advertenties, profilering of marktonderzoek.

Google treedt ook op als verwerkingsverantwoordelijke voor de aanvullende services binnen Google Workspace for Education. Voor het gebruik van onder andere YouTube, Google Search en Google Maps bepaalt Google doel en middelen van de verwerking van de persoonsgegevens.

⁷ https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-your-info

⁸ https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-your-info en <https://cloud.google.com/terms/cloud-privacy-notice-supplement>

Het afsluiten van een Service Data Addendum (SDA) is dus van fundamenteel belang voor Vlaamse schoolbesturen. Zonder dit addendum treedt Google op als verwerkingsverantwoordelijke voor servicegegevens, wat de controle van de school over de verwerking van persoonsgegevens ernstig ondermijnt en mogelijk in strijd is met de AVG-beginselen van doelbinding en verantwoordingsplicht. Het Service Data Addendum is de contractuele hefboom om de rol van Google als pure verwerker voor alle relevante data binnen de kernservices te garanderen en maakt deze afspraken juridisch bindend.

Verwerker

Indien het schoolbestuur geen Service Data Addendum met Google afsluit, treedt Google op als verwerker voor de 'klantgegevens' binnen de kernservices van Google Workspace for Education. Zij bieden het softwarepakket aan en verwerken de persoonsgegevens ('klantgegevens') in opdracht van de verwerkingsverantwoordelijke, in dit geval het schoolbestuur van de onderwijsinstelling(en).

Door een Service Data Addendum af te sluiten zorgt het schoolbestuur ervoor dat Google enkel als verwerker optreedt, voor zowel de klant- als de servicegegevens.

Subverwerkers

Alle informatie over de subverwerkers voor de kernservices van Google Workspace for Education is terug te vinden via Google Workspace Terms Of Service⁹.

Google kent subverwerkers voor drie type activiteiten: data center operations, service maintenance en technical support.

Google gebruikt subverwerkers uit derde landen waarmee niet altijd een adequaatheidsbesluit of andere standaard contractuele clausules mee werden afgesloten. Uit de analyse van de DPIA die in Nederland door SURF en SIVON werd uitgevoerd, blijkt dat Google de informatie over de subverwerkers wel heeft uitgebreid. Het is nu mogelijk om na te gaan welke persoonsgegevens de subverwerkers voor welke doeleinden kunnen inzien.

Chrome

Voor ChromeOS en de Chrome-browser met gegevensverwerkingsmodus (Data Processor Mode) op een beheerde Chromebook (essentiële diensten) is het schoolbestuur van de onderwijsinstelling(en) de verwerkingsverantwoordelijke voor zowel de klantgegevens als de servicegegevens. Google fungeert als verwerker voor "legitieme zakelijke doeleinden"¹⁰, zoals facturatie, accountbeheer, detectie van misbruik en het aanbieden van ondersteuning.

Bij ChromeOS en de Chrome-browser met gegevensverwerkingsmodus op een beheerde Chromebook (optionele diensten) is het schoolbestuur van de onderwijsinstelling(en) de verwerkingsverantwoordelijke, terwijl Google optreedt als verwerker. Dit is ook het geval wanneer men ChromeOS en Chrome-browser gebruikt zonder gegevensverwerkingsmodus.

Het is daarom belangrijk voor onderwijsinstellingen om de gegevensverwerkingsmodus voor ChromeOS en Chrome-browser in te schakelen. Op dat moment wordt het schoolbestuur van de onderwijsinstelling(en) de enige verwerkingsverantwoordelijke.

⁹ [Google Workspace Terms Of Service – Google Workspace](#)

¹⁰ <https://www.google.com/chrome/dpchromeos/eu/index.html>

6. Noodzakelijkheid en evenredigheid

6.1 De rechtmatigheid van de verwerking

Zoals vermeld in punt 5.3 is één van de sleutelcompetenties van de eindtermen die leerlingen moeten bereiken 'digitale competentie en mediawijsheid'. Deze sleutelcompetentie wordt zowel in het basisonderwijs (artikel 44, §2 van het decreet basisonderwijs) als in het secundair onderwijs (artikel 139, §2 van het Gecodificeerd Decreet betreffende het Secundair Onderwijs) omschreven. Leerlingen worden aangemoedigd om op een correcte en bewuste manier om te gaan met digitale hulpmiddelen en om de nodige digitale vaardigheden te ontwikkelen.

Onderwijsinstellingen hebben na zorgvuldige analyse gekozen om hiervoor gebruik te maken van Google Workspace for Education. Voor het gebruik van de kernservices van Google Workspace for Education geldt dat deze verwerking gebaseerd is op de vervulling van een taak van algemeen belang overeenkomstig artikel 6, lid 1, e) van de AVG.

Het wordt echter aanbevolen om het gebruik van Google Workspace for Education en de bijhorende verwerking van persoonsgegevens op te nemen in het privacybeleid van de onderwijsinstelling.

Het is belangrijk om te benadrukken dat deze rechtmatigheid enkel van toepassing is op het gebruik van de kernservices van Google Workspace for Education. De aanvullende services, zoals YouTube of Google Maps, voldoen niet aan deze rechtmatigheid aangezien Google bij het gebruik van deze services persoonsgegevens verwerkt voor eigen doeleinden (zoals commerciële profilering of productverbetering). Er is dus geen taak van algemeen belang om de aanvullende services te gebruiken.

Onderwijsinstellingen die de aanvullende services voor leerlingen inschakelen lopen het risico op onrechtmatige verwerking.

Voor het gebruik van de aanvullende services vraagt Google dat onderwijsinstellingen toestemming van ouders van leerlingen jonger dan 18 jaar moeten krijgen. Toestemming is in geen geval een geldige rechtsgrond voor het gebruik van aanvullende services.

Artikel 4, 11) AVG specificeert dat een toestemming gedefinieerd wordt "als elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt". In een situatie waarbij een ouder toestemming moet geven aan een onderwijsinstelling, kan deze toestemming echter niet als vrij beschouwd worden en kan dit ook niet als rechtsgrond aangewend worden.

6.2 De basisbeginselen van de verwerking

6.2.1 Behoorlijkheid en transparantie

Artikel 5, lid 1, a) van de AVG stelt dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.

Dit betekent dat de betrokkene op de hoogte moet zijn van de verwerking van zijn persoonsgegevens. De verwerkingsverantwoordelijke, in deze het schoolbestuur van de onderwijsinstellingen, zijn verplicht om leerlingen, ouders en personeelsleden van de onderwijsinstelling(en) te informeren over het volgende:

- de identiteit van de verwerkingsverantwoordelijke;
- welke persoonsgegevens verwerkt worden;
- met welk doel en op welke rechtsgrond de persoonsgegevens verwerkt worden;
- door wie de persoonsgegevens verwerkt worden;
- waar en hoe lang de persoonsgegevens bewaard worden;
- of en met wie de persoonsgegevens gedeeld worden;
- hoe betrokkenen hun rechten kunnen uitoefenen.

Deze informatie moet op toegankelijke wijze beschikbaar zijn via de privacyverklaring en/of het school- of centrumreglement, in duidelijke en begrijpelijke taal.

Het niet correct onderscheiden van kern- en aanvullende services en het ontbreken van transparante communicatie kan leiden tot schending van de AVG, met substantiële juridische en reputatierisico's tot gevolg. Deze GEB waarschuwt daarom expliciet voor het onvoldoende beheer van aanvullende Google-diensten binnen de onderwijscontext.

6.2.2 Doelbinding

Artikel 5, lid 1, b) van de AVG stelt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden.

In punt 5.2 van deze GEB wordt toegelicht welke doeleinden onderwijsinstellingen nastreven bij de verwerking van persoonsgegevens. Het gaat om verwerkingen binnen de primaire (onderwijskundige) en secundaire (ondersteunende) processen van een onderwijsinstelling, zoals opgenomen in het verwerkingsregister. De doeleinden zijn concreet, duidelijk omschreven en verenigbaar met de onderwijsopdracht van de instelling.

Hoewel de verwerkte persoonsgegevens noodzakelijk kunnen zijn voor het functioneren van de onderwijsinstelling, betekent dit niet automatisch dat verwerking via Google Workspace for Education ook noodzakelijk is. Elke onderwijsinstelling dient kritisch te beoordelen of het gebruik van deze persoonsgegevens binnen Google Workspace for Education strikt noodzakelijk is voor het beoogde doel.

Dit is des te belangrijker bij het verwerken van bijzondere persoonsgegevens (artikel 9 AVG), zoals gezondheidsgegevens of religieuze overtuigingen. Bij gebruik van bijvoorbeeld Google Forms of Gmail, en bij opslag in Google Drive, moet steeds worden afgewogen of de verwerking proportioneel is en in overeenstemming met de doelbinding. Onnodige opslag of uitwisseling van persoonsgegevens moet worden vermeden.

6.2.3 Minimale gegevensverwerking

Artikel 5, lid 1, c) van de AVG stelt dat persoonsgegevens toereikend moeten zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

Onderwijsinstellingen dienen ernaar te streven om enkel die persoonsgegevens te verwerken die

noodzakelijk zijn voor de primaire en secundaire onderwijsprocessen zoals vermeld in punt 5.2. Dit betekent dat enkel persoonsgegevens die 'need to know' zijn, verwerkt mogen worden. De verwerking van persoonsgegevens die 'nice to know' zijn, zoals bijvoorbeeld hobby's van leerlingen, moeten vermeden worden.

Toch werd tijdens de analyse opgemerkt dat er ook persoonsgegevens verwerkt kunnen worden die niet noodzakelijk zijn. Zo kunnen leerlingen bijvoorbeeld meer persoonsgegevens invullen dan noodzakelijk om een account voor Google Workspace for Education aan te maken. Het is aanbevolen om in de beveiligingsmaatregelen ervoor te zorgen dat betrokkenen enkel de noodzakelijke persoonsgegevens om een account aan te maken kunnen invullen.

Tijdens de analyse werd ook aandacht besteed aan de persoonsgegevens die kunnen verwerkt worden bij een inhoudelijke opdracht van een leerling. In een educatieve context moeten leerlingen zich vrij kunnen uitdrukken. Er wordt wel aangeraden om in de titel van een document en in het onderwerp van een e-mail geen persoonsgegevens te verwerken (zie ook punt 8).

6.2.4 Juistheid en nauwkeurigheid

Volgens artikel 5, lid 1, d) van de AVG moeten persoonsgegevens juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

De verwerkingsactiviteiten eisen dat de juistheid van de persoonsgegevens gegarandeerd kan worden en dat er voorzien wordt in een passend proces waarbij redelijke maatregelen voorzien worden om persoonsgegevens te wissen of te verbeteren in bepaalde situaties.

Dit kan mogelijk gemaakt worden door informatie op te halen uit andere schoolsystemen of door de persoonsgegevens rechtstreeks van de betrokkene te verkrijgen. Onderwijsinstellingen bekijken voor zichzelf welke maatregelen zij hiervoor nemen.

Deze aspecten komen ook nog aan bod in punt 8 bij de geïdentificeerde risico's.

6.2.5 Opslagbeperking

Artikel 5, lid 1, e) van de AVG stelt dat persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.

Bewaartermijn

De onderwijsregelgeving¹¹ legt voor een aantal leerlinggebonden documenten een uitdrukkelijke bewaartermijn op. Het gaat hier om documenten zoals het inschrijvingsregister, attesten ... Deze leerlinggebonden documenten worden niet noodzakelijk in Google Workspace for Education bewaard.

¹¹ [omzendbrief BaO/2005/03 van 31/01/2005](#)

Voor documenten die in Google Workspace for Education bewaard worden, dient de onderwijsinstelling zelf een bewaartermijn in te stellen. Google houdt informatie die verwijderd werd, nog maximaal 180 dagen na verwijdering bij¹².

6.2.6 Gegevensbeveiliging

Artikel 5, lid 1, f) stelt dat persoonsgegevens, door het nemen van passende technische of organisatorische maatregelen, op een dusdanige manier moeten worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Dit beginsel wordt tweeledig bekeken. Enerzijds wordt gekeken naar de beveiligingsmaatregelen die de onderwijsinstellingen kunnen nemen. Anderzijds wordt nagegaan welke beveiligingsmaatregelen Google zelf toepast.

Om digitale hulpmiddelen in het onderwijs te kunnen aanbieden, moet de onderwijsinstelling zorgen voor de goede werking van haar IT-systemen volgens het principe Vertrouwelijkheid, Integriteit en Beschikbaarheid. Dit betekent dat de onderwijsinstelling ervoor moet zorgen dat zij de passende technische en organisatorische maatregelen neemt om de veilige verwerking van persoonsgegevens te waarborgen.

Leerlingen en ouders hebben geen keuze in de verwerking van hun persoonsgegevens in Google Workspace for Education. De onderwijsinstelling maakt deze keuze voor hen. Het is daarom heel belangrijk om de correcte beveiligingsmaatregelen in te stellen in Google Workspace for Education.

Dit kan gaan om volgende maatregelen die kunnen genomen worden:

- Instellen van de juiste rollen: lees- en schrijfrechten
- Instellen van de mogelijkheid om documenten al dan niet te downloaden, afdrukken of kopiëren
- Implementeren van een correct toegangsbeheer, bijvoorbeeld via 2-stapsverificatie
- Implementeren van een toereikend wachtwoordbeleid
- Instellen van de nodige beveiligingsmaatregelen i.h.k.v. het delen van documenten
- Instellen van de correcte bewaartermijn
- Sensibiliseren van leerlingen en personeelsleden van de onderwijsinstelling

Kenniscentrum Digisprong werkte een technische handleiding uit om de nodige beveiligingsmaatregelen in te stellen voor Google Workspace for Education. Deze handleiding is terug te vinden in bijlage 3.

Hoewel het noodzakelijk is dat onderwijsinstellingen de nodige beveiligingsmaatregelen in Google Workspace for Education instellen, voorziet Google zelf ook beveiligingsmaatregelen¹³.

- Encryptie van data at rest, data in transit en data in use
- Instellen van toegangsrechten voor werknemers die enkel noodzakelijke toegang nodig hebben
- Geografische verdeling van de datacenters
- Disaster recovery testing

¹² [GDPR and Google Cloud | Google Cloud](#)

¹³ [GDPR and Google Cloud | Google Cloud](#)

6.3 Noodzakelijkheid en evenredigheid

6.3.1 Noodzaak

De verwerkingsverantwoordelijke geeft aan waarom de verwerkingen noodzakelijk zijn voor de vooropgestelde doeleinden.

6.3.2 Evenredigheid

Een alternatief voor Google Workspace for Education zou het gebruik van een softwarepakket bij een Europese cloudprovider kunnen zijn.

Om persoonsgegevens nog beter te beschermen, is het aan te raden om over te schakelen naar de betalende versie, namelijk Google Workspace for Education Standard of Plus. Deze versie biedt meer mogelijkheden om beveiligingsmaatregelen in te stellen, zoals het opslaan van gegevens op een Europese server.

Het is de taak van de verwerkingsverantwoordelijke om te onderbouwen dat het gebruik van Google Workspace for Education een noodzakelijke en proportionele keuze is voor de uitvoering van de primaire en secundaire onderwijsprocessen. Daarbij moet de verwerkingsverantwoordelijke aangeven of en in welke mate er is nagedacht over mogelijke alternatieven en waarom deze minder geschikt zijn.

6.4 Internationale doorgifte

Datacenters buiten EER

Google Workspace for Education wordt aangeboden door Google. Het hoofdkantoor van Google is gevestigd in de Verenigde Staten en bevindt zich daarmee buiten de Europese Economische Ruimte (EER). Hierdoor is er mogelijk sprake van internationale doorgifte van persoonsgegevens. In 2023 heeft de Europese Commissie een adequaatheidsbesluit aangenomen tot vaststelling van het EU-US Data Privacy Framework. Daarin heeft de Commissie vastgesteld dat de Verenigde Staten een passend beschermingsniveau waarborgen voor persoonsgegevens die vanuit de EER worden doorgegeven aan organisaties die zijn opgenomen in het Data Privacy Framework.

Google is één van de organisaties die zich heeft gecertificeerd binnen het EU-US Data Privacy Framework. Dit biedt verschillende waarborgen en mechanismen die specifiek zijn ontworpen om de privacy van betrokkenen binnen de EER te beschermen bij de overdracht van persoonsgegevens naar de Verenigde Staten.

Toch biedt het adequaatheidsbesluit geen volledige zekerheid op het gebied van gegevensbescherming. Zo hebben EU-burgers geen effectieve rechtsbescherming tegen de Amerikaanse surveillance. EU-burgers weten vaak niet dat hun gegevens zijn verzameld of kunnen daartegen geen bezwaar maken of beroep instellen. Persoonsgegevens van EU-burgers worden opgeslagen of verwerkt door Amerikaanse bedrijven zoals Google, en zijn daarvoor mogelijk toegankelijk voor Amerikaanse inlichtingendiensten.

De bescherming van persoonsgegevens is grotendeels gebaseerd op het uitvoeringsbesluit Executive Order 14086. Dit Executive Order probeert bovenstaande problemen aan te pakken en stelt dat Amerikaanse overheidsinstanties, zoals de FBI, persoonsgegevens van EU-burgers (en burgers uit andere landen) enkel

mogen verzamelen indien dit noodzakelijk en proportioneel is voor nationale veiligheidsdoeleinden. Er is tevens een klachtenmechanisme voorzien voor burgers uit andere landen, waaronder EU-burgers, die menen dat hun gegevens onrechtmatig verzameld zijn door Amerikaanse inlichtingendiensten.

Desondanks blijven er juridische twijfels over de mate van bescherming en duurzaamheid van het systeem. Bovendien zou, tegen de achtergrond van de huidige geopolitieke situatie, dit uitvoeringsbesluit mogelijk kunnen worden gewijzigd of ingetrokken, hetgeen tot onzekerheid leidt.

Hoewel het adequaatheidsbesluit een tijdelijke juridische basis biedt voor gegevensoverdracht, blijven de fundamentele structurele verschillen in wetgeving betreffende de bescherming van persoonsgegevens en onzekerheden voor juridische bescherming bestaan.

Google publiceert in haar Transparency Report¹⁴ gedetailleerde informatie over het aantal verzoeken dat zij ontvangt van overheden, waaronder de Amerikaanse, om gebruikersgegevens te verstrekken, inclusief hoe vaak en in welke mate op die verzoeken wordt ingegaan.

Betalende versie

Ten opzichte van de momenteel beschikbare technische handleiding (bijlage 3) raden we ten eerste aan om persoonsgegevens uitsluitend op servers binnen de Europese Economische Ruimte op te slaan, om het risico op ongecontroleerde gegevensdoorgifte te beperken. Deze mogelijkheid wordt enkel geboden binnen de betalende versies van Google Workspace for Education Standard of Plus¹⁵.

Omwille van de extra functionaliteiten en beveiligingsmaatregelen die Google Workspace for Education Standard of Plus aanbiedt, wordt aangeraden om één van deze betalende versies te gebruiken. Deze versies bieden de mogelijkheid om de gegevensverwerking volledig op datacenters binnen de Europese Economische Ruimte te laten plaatsvinden. Hierdoor krijgen onderwijsinstellingen meer grip op de geografische locatie van de dataopslag én de juridische bescherming die daaraan verbonden is.

Voor de Plus-versie kan een meerjarencontract worden afgesloten, terwijl de Standard-versie uitsluitend in de vorm van een jaarcontract beschikbaar is. Op het gebied van beveiliging voldoen beide versies aan de momenteel gestelde eisen.

Met Google Workspace for Education Standard of Plus kan de onderwijsinstelling:

- de afhankelijkheid van het EU-US Data Privacy Framework sterk verminderen;
- de compliance versterken met de beginselen van doelbinding, dataminimalisatie en opslagbeperking onder de AVG;
- het risico op inbreuken bij internationale doorgifte en onrechtmatige toegang door buitenlandse overheden aanzienlijk verlagen.

De keuze voor Google Workspace for Education Standard of Plus is daarom geen louter functionele of commerciële overweging, maar een actieve maatregel ter bescherming van de rechten van leerlingen, personeelsleden en ouders, én een blijk van verantwoord gegevensbeheer.

¹⁴ [Verzoeken om gebruikersgegevens – Transparantierapport van Google](#)

¹⁵ [Google Workspace-versies vergelijken - Education](#)

7. Methode voor beoordeling risico's op rechten en vrijheden van betrokkenen

7.1 Aanvaardbaarheidscriteria van negatieve effecten

De aanvaardbaarheidscriteria zijn gekoppeld aan de score die wordt toegekend aan een risico op basis van een combinatie van twee aspecten: de impact van het risico en de waarschijnlijkheid van het risico.

- Risico's met een score **“hoog”** of **“kritiek”** kunnen niet geaccepteerd worden zonder bijkomende risicomaatregelen.
- Risico's met een score **“gemiddeld”** worden idealiter nog verder behandeld. Het is mogelijk (en in bepaalde gevallen aangewezen) om hier nog bijkomende risicomaatregelen te nemen. Indien geen mogelijke aanvullende maatregelen voorhanden zijn, of bv. de kost van de maatregel niet in proportie tot het risico staat, kunnen deze risico's geaccepteerd worden mits duidelijke en grondige motivatie.
- Risico's met een score **“laag”** en **“zeer laag”** kunnen zonder bijkomende motivering geaccepteerd worden.

De cijferscores in het document dienen als volgt gelezen te worden:

- 1-4: laag tot zeer laag
- 5-9: gemiddeld
- 10-16: hoog
- 20-25: kritiek

7.2 Risicoanalyse, -evaluatie en opvolging

In Nederland werd een onderzoek uitgevoerd naar de risico's met betrekking tot de bescherming van persoonsgegevens bij het gebruik van Google Workspace for Education. Dit onderzoek bracht risico's aan het licht die verband houden met accountgegevens, ondersteuningsgegevens en diagnostische gegevens. Na overleg heeft Google de nodige maatregelen genomen en wijzigingen doorgevoerd in Google Workspace for Education en in de Google Cloud Privacyverklaring (Privacy Amendment). Google heeft aan de Vlaamse Toezichtcommissie laten weten dat equivalente voorwaarden en gegevensbeschermingsmaatregelen voor het Vlaamse onderwijs zullen gelden als voor het Nederlandse onderwijs.

In deze GEB zullen de bovengenoemde risico's dan ook niet meer worden onderzocht, maar worden de risico's in kaart gebracht die verband houden met de verwerkingsactiviteiten van onderwijsinstellingen. In bijlage 4 is een lijst van aanbevelingen (zie ook bijlage 3 Technische handleiding) opgenomen zodat de onderwijsinstellingen de nodige maatregelen kunnen nemen om de geïdentificeerde risico's tot een minimum te herleiden.

7.2.1 Bepalen van de impact van een risico voor betrokkene

Om het impactniveau op de betrokkene te bepalen moet rekening gehouden worden met de rechten en vrijheden van de betrokkene, alsook met de gerechtvaardigde belangen zowel op economisch, fysiek of psychologisch vlak, zoals onder meer:

- Een mogelijk verlies aan zelfstandigheid (potentiële handelingen kunnen niet meer worden uitgevoerd);
- Vrij kunnen blijven van stigmatisering (hoe de betrokkene behandeld wordt op basis van bepaalde kenmerken);
- Gelijkheid (het op dezelfde wijze benaderen van de betrokkene);
- Bewegingsvrijheid (beperken van toegang tot bepaalde ruimtes of locaties);
- Vrij kunnen blijven van manipulatie (beïnvloeden van het gedrag op basis van de geschonden informatie);
- Integriteit (bv. door aanbieden van geschenken);
- Ongestoord leven (onaangenaam afbreken van rust en stilte);
- Eigenwaarde (afbreuk aan eigen persoonlijkheid);
- Autonomie (beperking van de vrijheid om eigen regels te volgen);
- Lichamelijke schade en bedreigingen;
- Identiteitsfraude;
-

Impact	Score	Impact gegevensbescherming
Kritiek	5	De betrokkene lijdt zeer ernstige en permanente schade.
Significant	4	De betrokkene lijdt ernstige schade die moeilijk recht te zetten is.
Groot	3	De betrokkene lijdt aanzienlijke schade die niet snel recht te zetten is.
Gemiddeld	2	De betrokkene kan schade lijden, maar die is snel recht te zetten.
Klein	1	Er is geen enkele of slechts een verwaarloosbare impact op de betrokkene.

7.2.2 Bepalen van de waarschijnlijkheid van een risico voor betrokkene

Waarschijnlijkheid	Score	Kans – in cijfers	Omschrijving	Frequentie
Voorzienbaar	5	> 90%	Een gebeurtenis waarvan het zo goed als zeker is dat ze zal plaatsvinden.	1x per maand of vaker
Hoog	4	60% - 90%	Een gebeurtenis waarvan de kans groot is dat ze zal plaatsvinden.	1x per kwartaal
Gemiddeld	3	30% - 60%	Dit is al eerder voorgekomen, en is ook nu mogelijk.	1x per jaar
Laag	2	10% - 30%	Het gaat om een zeldzame gebeurtenis.	1x per 1 à 5 jaar
Zeer laag	1	< 10%	Dit is niet echt van toepassing in de huidige	Minder dan 1x per 5 jaar

context.

7.2.3 Bepalen van de risicomatrix

Aan de hand van het bepalen van de waarschijnlijkheid en impact van een risico wordt een risicokaart opgesteld. Deze kaart geeft inzicht in de spreiding van de risico's naar waarschijnlijkheid en impact. Dit laat toe om de risico's te prioriteren zodat de belangrijkste eerst aangepakt worden.

WAARSCHIJNLIJKHEID (kans/frequentie)	5	Voorzienbaar Het is te verwachten dat een risico in dit domein zich meerdere keren per kwartaal zal voordoen	5	10	15	20	25
	4	Hoog Het is te verwachten dat een risico in dit domein zich meerdere keren per jaar zal voordoen	4	8	12	16	20
	3	Gemiddeld Het is te verwachten dat een risico in dit domein zich minstens 1 keer per jaar zal voordoen	3	6	9	12	15
	2	Laag Het is te verwachten dat een risico in dit domein zich minstens 1 keer per decennium zal voordoen	2	4	6	8	10
	1	Zeer Laag Het is te verwachten dat een risico in dit domein zich minder dan 1 keer per decennium zal voordoen	1	2	3	4	5
			IMPACT (gevolg/ernst)				
			1	2	3	4	5
			Klein	Gemiddeld	Groot	Significant	Kritiek

Kritiek risico	Het risico is niet aanvaardbaar en kan niet geaccepteerd worden zonder bijkomende maatregelen.
Hoog risico	Het risico is niet aanvaardbaar en kan niet geaccepteerd worden zonder bijkomende maatregelen.
Gemiddeld risico	Het risico wordt idealiter nog verder behandeld. Het is mogelijk (en in bepaalde gevallen aangewezen) om hier nog bijkomende risicomaatregelen te nemen. Indien geen mogelijke aanvullende maatregelen voorhanden zijn, of bv. de kost van de maatregel niet in proportie tot het risico staat, kunnen deze risico's geaccepteerd worden mits duidelijke en grondige motivatie.
Laag risico	Het risico kan zonder bijkomende motivering geaccepteerd worden.

8. Beoordeling risico's op rechten en vrijheden van betrokkenen

De noodzaak voor de uitvoering van een GEB insinueert een context waarbinnen een verwerking gelet op de aard, de omvang, de context en de doeleinden waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

In deze GEB wordt telkens een risico besproken, welke aanvullende maatregelen er genomen worden, alsook welke beoordeling geleid heeft tot een score van het restrisico.

De uitgebreide risicoanalyse is terug te vinden in bijlage 2.

9. Beoogde maatregelen om risico's aan te pakken

De beoogde maatregelen om de beschreven risico's aan te pakken zijn omschreven in bijlage 2 en 3 van deze GEB.

In bijlage 4 kan de verwerkingsverantwoordelijke invullen welke maatregelen al dan niet geïmplementeerd worden en wat de planning voor implementatie is.

Als de verwerkingsverantwoordelijke ervoor kiest om één of meerdere van de maatregelen niet te implementeren, dan heeft dit gevolgen voor de afweging van de privacyrisico's. Het is dan aan de verwerkingsverantwoordelijke om te onderbouwen dat het niet nemen van de technische maatregel(en) geen gevolgen heeft voor de risico's en/of wat de compenserende maatregelen zijn die de onderwijsinstelling neemt om het privacyrisico van het gebruik van Google Workspace for Education niet te laten toenemen.

10. Mening betrokkenen/vertegenwoordigers over de verwerking

Bij het opstellen van deze white label GEB werd er gesproken met vertegenwoordigers uit het onderwijsveld die ervaring hebben met het gebruik van Google Workspace for Education. De GEB omvatte geen directe bevraging van betrokkenen.

De verwerkingsverantwoordelijke is vrij om, als zij dit wenselijk acht, eigen betrokkenen (zoals leerlingen, ouders of personeelsleden) te bevragen. De resultaten hiervan kunnen in dit onderdeel opgenomen worden.

11. Adviezen betreffende de GEB

11.1 Advies functionaris voor gegevensbescherming

De verwerkingsverantwoordelijke noteert hier het advies van de functionaris voor gegevensbescherming.

11.2 Voorafgaande raadpleging bij de toezichthouder (verplicht bij hoog restrisico)

Indien er een hoog restrisico zou zijn en de verwerkingsverantwoordelijke vraagt advies bij de toezichthouder, wordt deze reactie hieronder beschreven.

11.3 Overzicht van de acties die de verwerkingsverantwoordelijke neemt naar aanleiding van het advies van de functionaris en de raapleging van de toezichthouder

De verwerkingsverantwoordelijke noteert hier welke maatregelen zullen genomen worden naar aanleiding van bovenstaande adviezen.

12. Besluit van de verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke noteert hier het besluit betreffende de verwerking van persoonsgegevens in Google Workspace for Education.

Op basis van de risicoanalyse in het kader van de white label GEB wordt geconcludeerd dat de gevolgen voor de rechten en vrijheden van de betrokkenen (leerlingen, ouders en personeelsleden) bij de verwerking van persoonsgegevens in Google Workspace for Education, na toepassing van de risicobeperkende maatregelen, in [voldoende/onvoldoende] mate beheerst zijn.

De reeds genomen en nog te implementeren maatregelen binnen Google Workspace for Education zijn [voldoende/onvoldoende] afgestemd op het beperken van de risico's voor de rechten en vrijheden van betrokkenen.

Er is [wel/niet] vastgesteld dat er nog hoge risico's blijven bestaan die een 'voorafgaande raadpleging' bij de Vlaamse Toezichtcommissie (conform artikel 36 AVG) noodzakelijk maken.

[VERWERKINGSVERANTWOORDELIJKE VAN NAAM ONDERWIJSINSTELLING(EN)] verklaart hierbij:

- kennis te hebben genomen van de inhoud van de white label GEB;
- de (rest)risico's te aanvaarden;
- opdracht te geven voor het implementeren van de aanbevolen maatregelen;
- deze GEB na een periode van twee jaar te herbekijken, of eerder indien nodig;
- [wel/geen] voorafgaande raadpleging bij de Vlaamse Toezichtcommissie in te dienen.

Tot slot besluit [VERWERKINGSVERANTWOORDELIJKE VAN NAAM ONDERWIJSINSTELLING(EN)] het gebruik van Google Workspace for Education Fundamentals [wel/niet] voort te zetten, en [wel/niet] over te schakelen naar een betalende versie, zijnde Google Workspace for Education Standard of Plus.

Naam verwerkingsverantwoordelijke:

Naam bestuurder(s):

Plaats:

Datum:

Handtekening

Bijlagen

- Bijlage 1: Verwerkingsactiviteiten en persoonsgegevens
- Bijlage 2: Risicoanalyse Google Workspace for Education
- Bijlage 3: Technische handleiding Google Workspace for Education Kenniscentrum Digisprong
- Bijlage 4: Beoogde maatregelen om risico's aan te pakken

Bronnen

- Privacy in onderwijs, 19 februari 2024, www.privacyinonderwijs.be
- Onderwijsdoelen, <https://onderwijsdoelen.be>
- Kernservices en aanvullende services van Google Workspace for Education, [Kernservices en aanvullende services van Google Workspace for Education](#)
- Google Workspace for Education data protection implementation guide, februari 2023, [Google workspace edu data protection implementation guide.pdf](#)
- Privacyverklaring voor Google Workspace for Education, https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-your-info
- Addendum voor gegevens in de Google Workspace for Education-service, <https://workspace.google.com/terms/service-data-addendum/>
- Aanvullende privacyverklaring van Google Cloud, 7 december 2023, <https://cloud.google.com/terms/cloud-privacy-notice-supplement>
- Google Workspace en cloud subverwerkers, 5 juni 2025, <https://workspace.google.com/terms/subprocessors/>
- ChromeOS Overeenkomst gegevensverwerkersmodus, <https://www.google.com/chrome/dpchromeos/eu/index.html>
- Bewaartermijn van leerlinggebonden documenten, 20 augustus 2018, <https://data-onderwijs.vlaanderen.be/edulex/document.aspx?docid=13572>
- Google Cloud & the General Data Protection Regulation (GDPR), augustus 2021, <https://cloud.google.com/privacy/gdpr?hl=nl>
- Google Workspace-versies vergelijken, [Google Workspace-versies vergelijken](#)
- Google Transparantierapport, Verzoeken om gebruikersgegevens met betrekking tot de nationale veiligheid in de Verenigde Staten, <https://transparencyreport.google.com/user-data/us-national-security>