Technische handleiding voor Google Workspace for Education

Versie 3.0 februari 2024

Inhoudsopgave

2 augustus 2021 (versie 1.0)	*Eerste versie van de technische handleiding met daarin beschrijving van Google Workspace instellingen die scholen moeten doorvoeren om privacy risico's uit de update DPIA augustus 2021 te mitigeren.*
20 juli 2023 (versie 2.0)	*In de periode augustus 2021 tot juni 2023 heeft Google diverse privacy verbeteringen doorgevoerd in Workspace. Ondanks de aanpassingen door Google blijven alle maatregelen uit 2021 van toepassing. In versie 2 van de technische handleiding wordt nu verwezen naar de actuele stand van zaken zoals bekend na de verificatie van de genomen maatregelen door Google.* *Versie 2 bevat aanvullende informatie over Cookies en Youtube.*
31 augustus 2023 (versie 2.1)	*Toevoeging versie beheer tabel en wijzigingen in opmaak*
27 februari 2024 (versie 3.0)	*Update naar aanleiding van DTIA*

1 Introductie

In 2021 is er een privacyonderzoek uitgevoerd op Workspace for Education (in 2021 G Suite for Education genoemd). Uit deze *data protection impact assessment* (DPIA) bleek dat er hoge privacyrisico's kleefden aan het gebruik van Google Workspace for Education.

SIVON en SURF, coöperaties van en voor onderwijs- en onderzoeksinstellingen in Nederland, hebben naar aanleiding van het onderzoek in 2021 afspraken gemaakt met Google om de geconstateerde privacyrisico's te verminderen. Google is de afspraak nagekomen en heeft de nodige maatregelen genomen en wijzigingen doorgevoerd in de software. Deze zijn medio 2023 door SIVON en SURF en de door hen ingeschakelde externe privacyexperts gecontroleerd. Deze uitkomsten zijn opgenomen in het "*Verification report Google remediation measures Workspace for Education*" van Privacy Company (dd 15 juni 2023).

Naast de aanpassing die Google doorgevoerd heeft moeten onderwijsinstellingen zelf ook maatregelen nemen om de risico's te beperken. Het gaat om instellingen die beheerders (*admins*) kunnen wijzigen in Google Workspace for Education en wijzigingen die gebruikers zelf kunnen doen.

Tevens bevat deze handleiding maatregelen die gericht zijn op het gebruik van Chrome devices en Chrome browser. In 2023 is het privacy onderzoek naar Chrome afgerond. Naar aanleiding van dit onderzoek zijn er aanvullende maatregelen beschreven.

Tot slot is er in 2023 een DTIA uitgevoerd op Google Workspace for Education (Google meet). Met een DTIA worden de risico's van internationale doorgifte in kaart gebracht. Internationale doorgifte risico is in DPIA uit 2021 toegevoegd nadat de Schrems II uitspraak de EU-VS Data Protection Shield ongeldig verklaard heeft. In de DPIA is dat risico 9. In versie 3.0 van deze handleiding zijn de maatregelen beschreven die moeten worden genomen om risico's van internationale doorgifte te beperken. De maatregelen staan beschreven in hoofdstuk 7.

Alle in deze handleiding genoemde handelingen zijn privacy-bevorderende maatregelen die meegewogen zijn bij het beperken van de risico's van het gebruik van Workspace for Education (Plus) in het onderwijs. Indien een onderwijsinstelling besluit één of meerdere van de maatregelen niet te implementeren, dan heeft dit gevolgen voor de afweging van de privacyrisico's. De onderwijsinstelling moet dan zelf onderbouwen dat het niet nemen van de technische maatregel geen gevolgen heeft voor de privacyrisico's en/of wat de compenserende maatregelen zijn die de onderwijsinstelling neemt om het privacyrisico van het gebruik van Workspace for Education niet te laten toenemen. Het niet opvolgen van de technische maatregelen is dus niet zonder gevolg en moet nadrukkelijk beschreven en getoetst worden door de functionaris voor gegevensbescherming.

Verscheidene producten of functionaliteiten van Google Workspace for Education werken door (potentieel) privacygevoelige data te delen met Google. In deze handleiding wordt uitgelegd hoe je de data kunt minimaliseren door het aanpassen van instellingen voor gebruikersaccounts en producten. We leggen uit welke maatregelen je moet nemen, waarom dit nodig is en hoe je dit kunt uitvoeren.

Deze handleiding maakt onderdeel uit van drie stappen die scholen zelf moeten uitvoeren voordat zij Google Workspace for Education kunnen (blijven) gebruiken:

1. Accepteren gewijzigde voorwaarden Education Agreement Workspace for Education.
2. Deze technische stappen doorlopen en uitvoeren.
3. Uitvoeren onderwijsspecifieke DPIA (op basis van de handreiking lokale DPIA van SURF, SIVON en Kennisnet).

2 Algemene adviezen en informatie

2.1 Informatievoorziening medewerkers, leerlingen, studenten en hun ouders

Het verdient de voorkeur om bij het begin van het schooljaar jouw medewerkers, leerlingen, studenten en hun ouders te informeren over het gebruik van Google Workspace for Education en de gekozen privacy-instellingen. SIVON stelt hiervoor voorbeeldbrieven voor medewerkers en ouders beschikbaar. Het gaat hierbij specifiek om informatie over de verwerking van gegevens door Google, de afspraken van de onderwijsinstelling met Google en 'high level information' over de risico's van het gebruik van Workspace for Education. Dit laatste betekent dat de afspraken met Google alleen gelden zolang medewerkers, leerlingen en studenten ingelogd zijn in hun account en niet met een privé-account bij Google. Het is belangrijk om leerlingen en studenten erop te wijzen dat als hun profielfoto verdwijnt uit hun account, dit betekent dat ze de beschermde Workspace for Education-omgeving hebben verlaten.

Verder geldt het algemene advies aan medewerkers, leerlingen en studenten om zo min mogelijk (bijzondere) persoonsgegevens op te nemen in hun accountinformatie en in de informatie die zij met anderen delen.

2.2 Inzageverzoeken

Medewerkers, leerlingen en studenten die meer informatie willen over de gegevens die Google van en over hen verwerkt, kunnen bij hun onderwijsinstelling via de Administrator van Workspace for Education informatie opvragen. Als een medewerker, leerling of student klaagt dat het antwoord op diens inzageverzoek onvolledig is beantwoord, dan is het argument van Google dat zij zich beroept op de uitzondering van de AVG dat er geen inzage wordt gegeven als de betrokkene niet kan worden geïdentificeerd. Alleen de onderwijsinstelling en niet Google kan gebruikers identificeren. Bij het uitblijven van identificatie van de gebruiker, stelt Google geen informatie te mogen verstrekken over de betrokkenen.

2.3 Doorgifte van persoonsgegevens naar derde landen

In 2023 is de *data transfer impact assessment* (dtia) afgerond zoals dat beschreven is in de adviezen van de Autoriteit Persoonsgegeven (AP) en de EDPB. Accepteer de (nieuwe) standard contractuele clausules van Google https://cloud.google.com/security/compliance/eu-scc. De uitkomsten van de dtia worden beschikbaar gesteld zodra deze is afgerond door SURF en SIVON. Meer informatie over doorgifte van persoonsgegevens lees je in het artikel Aanbevelingen voor doorgifte data naar onveilige landen definitief.

2.4 Subverwerkers

Een van de risico's is het gebrek aan informatie over de leveranciers van Google (subverwerkers). Google gebruikt subverwerkers voor drie type activiteiten (doelbinding).

Data Center Operations: Beheer van het Google datacenter waar opslag van klantdata plaatsvindt. De subverwerker heeft geen toegang tot klantdata.

Service Maintenance: Subverwerker voor technisch onderhoud en probleemoplossing op software en hardware. De subverwerker kan beperkt toegang nodig hebben tot klantdata om technische problemen op te lossen.

Technical Support: Als een schoolbestuur een supportvraag heeft komt deze bij een subverwerker terecht. De subverwerker heeft toegang tot de data die het schoolbestuur meestuurt met een supportvraag.

Informatie over subverwerkers van Google is te vinden op deze pagina.

2.5 Meer informatie over privacy

Meer informatie over Chrome privacy is te vinden in de Google Chrome Privacy Whitepaper. https://www.google.com/chrome/privacy/whitepaper.html

Meer informatie over welke adviezen Google geeft voor nakoming van de AVG is te vinden in de Google Workspace Edu Data Protection Implementation Guide. https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf

2.6 Scope

De gewijzigde voorwaarden Education Agreement Workspace for Education is alleen van toepassing op de zogenaamde core services (zoals Gmail, Google Calendar, Doc, Drive and Classroom. De volledige lijst https://workspace.google.com/intl/en/terms/user_features.html

Additionele services (zoals Youtube, Google maps, Blogger, etc.) vallen buiten de scope van de overeenkomst.

3 Overzicht maatregelen

De onderwijsinstelling dient verscheidene functionaliteiten van Google Workspace for Education op een specifieke wijze in te stellen of uit te zetten. In onderstaande tabel is een overzicht opgenomen van de maatregelen die je moet nemen en de bijbehorende wijze van beheer. In de volgende hoofdstukken worden de maatregelen verder toegelicht inclusief informatie over implementatie.

Naar Chromebooks is een aanvullend privacy onderzoek gedaan. De resultaten daarvan zijn op 3 juli 2023 gepubliceerd. https://sivon.nl/2023/07/sivon-surf-en-google-bereiken-overeenkomst-terms-of-service-google-chrome/

3.1 Structuur

De indeling van de maatregelen is als volgt

Er zijn drie manieren van implementatie voor de te nemen maatregelen:

- Centraal beheer van devices en browsers (device management)
- Centraal beheer van instellingen via Google Workspace Admin console.
- Centraal beheer van instellingen via groepsbeleid (Group Policy) van het besturingssysteem.
- Individuele instellingen.

Maatregelen die dataminimalisatie bij het gebruik van producten of functionaliteiten betreffen kunnen ofwel via de Admin console, ofwel via het groepsbeleid van het besturingssysteem geïmplementeerd worden.

Tot slot bevat deze handleiding ook generieke maatregelen. Dit zijn maatregelen die niet specifiek zijn voor Google, maar in algemene zin ook nuttig zijn om privacy risico's te beperken. Deze maatregelen zijn:

- Gebruik van Youtube vanaf andere platformen.
- Beleid rondom cookies.
- Instrueer gebruikers over gebruik van privacygevoelige informatie in file en folder namen.
- Het geen gebruik maken van echte namen van medewerkers, leerlingen of studenten in email adressen.
- Installeer een browserextensie die tracking blokkeert.
- Gebruik een privacyvriendelijke zoekmachine, zoals DuckDuckGo of Startpage.

3.2 Maatregelen betreffende gebruikersaccounts

Gebruikersprofiel	K-12 profiel instellen voor alle gebruikers
Gebruikersdata	Geen gebruik maken van echte namen van medewerkers, leerlingen of studenten in emailadressen
	Gebruikers verbieden profiel zelf aan te passen
Geografische locatie dataopslag	Google Cloud opslaglocatie aanpassen naar Europa indien mogelijk
Aanvullende Google diensten	Uitzetten van aanvullende Google-services. Ook als je geen Google Workspace gebruikt, zitten er privacyrisico's aan het gebruik van aanvullende Google services zoals YouTube.
Google Workspace Marketplace-apps	Gebruikers niet toestaan apps uit de Google Workspace Marketplace te installeren
Nieuwe Google producten	Nieuwe producten niet automatisch beschikbaar te stellen voor gebruikers

3.3 Maatregelen betreffende dataminimalisatie in producten en functionaliteiten

Product of functionaliteit	Admin console instelling	Besturingssysteem groepsbeleid
Spellingcontrole	Lokale spellingcontrole kan aan staan	SpellCheckEnabled: true
Spellingcontrole Webservice	Webservice voor spellingcontrole uitzetten	SpellCheckServiceEnabled: false
Chromebrowser	Chrome synchronisatie niet toestaan	ClearBrowsingDataOnExitList SyncDisabled
Automatische vertaling websites	Nooit een vertaling voorstellen	TranslateEnabled: false
Geolocatie	Niet toestaan dat sites de geolocatie van gebruikers vaststellen	DefaultGeolocationSetting: 2
Gebruikersfeedback formulier	Gebruikersfeedback niet toestaan	UserFeedbackAllowed: false
Rapportage van statistieken	Anonieme gebruikersrapporten en rapporten met gegevens over crashes nooit naar Google sturen	MetricsReportingEnabled: false
Nieuw Tabblad Contentsuggesties	Geen contentsuggesties weergeven op de pagina Nieuw tabblad	NTPCardsVisible: false
Tabblad promotionele content	Weergave promotionele content op volledig tabblad uitschakelen	PromotionalTabsEnabled: false
Nieuw Tabblad Kaarten	Kaarten niet weergeven op de pagina Nieuw Tabblad	NTPContentSuggestionsEnabled : false
Search suggested service	Gebruikers nooit toestaan search suggest te gebruiken	SearchSuggestEnabled: false

Inloggen op secundaire accounts	Gebruikers alleen toestaan met een account op het schooldomein in te loggen	SecondaryGoogleAccountSigninAllowed: false
Cookies	Cookies van derden blokkeren	BlockThirdPartyCookies: true
Cookies	Cookies alleen bewaren voor de duur van de sessie	DefaultCookieSettings: 4
Systeemrapportages van bezochte pagina's	Het verzenden van aanvullende gegevens om Safe Browsing te helpen verbeteren, uitschakelen	SafeBrowsingExtendedReportingEnabled: false
Chrome Cleanup	Niet toestaan periodiek te scannen of Resultaten van Chrome Cleanup worden nooit gedeeld met Google	ChromeCleanupEnabled: false - OF - ChromeCleanupReportingEnabled: false

3.4 Individuele maatregelen en instructies

Advertentiepersonalisatie	Individueel instellen, indien er géén sprake is van een K-12 gebruikersprofiel.
YouTube video embedding	Gebruik alleen embedded video's met 'privacy-enhanced mode'.
Gebruik geen Chrome browser	Gebruik een alternatieve browser, totdat de nieuwe versie uitkomt waar Google als data verwerker optreedt.
Gebruik Google niet als zoekmachine	Gebruik een privacyvriendelijke zoekmachine, zoals DuckDuckGo of Startpage.
Gebruik een advertentie- en/of tracking blocker	Installeer een browserextensie die tracking blokkeert.
Gebruik geen privacy gevoelige informatie in file en folder namen	Instrueer gebruikers over privacygevoelige informatie in file en folder namen

4 Centrale beheeropties mogelijk maken

4.1 Onder beheer plaatsen van Chromebooks en Chromebrowsers

Beheerders van Google Workspace hebben een type account waarmee veel controle kan worden uitgeoefend op de data die met Google gedeeld wordt. De meeste maatregelen kunnen gecentraliseerd vanuit de Google Workspace Admin console beheerd worden.

Om dit mogelijk te maken moeten de Chromebooks en Chromebrowsers van een organisatie ook daadwerkelijk onder beheer geplaatst zijn. De Chromebooks en Chromebrowsers moeten hiervoor aangemeld zijn bij uw organisatie en desbetreffende organisatie-eenheid binnen Google Workspace. Deze nemen vervolgens alle instellingen over die je in de Google Workspace Admin console aangeeft.

Bij Chromebooks dient het gehele apparaat onder beheer gesteld te worden. Bij de besturingssystemen Windows, Mac en Linux dient de Chromebrowser onder beheer geplaatst te worden. Hieronder volgen de instructies om dit te bewerkstelligen.

4.2 Chromebooks onder beheer brengen

Chromebooks onder beheer brengen gebeurt veelal via jouw leverancier. Voor centraal beheer van Chromebooks heb je de Chrome Education Upgrade licentie nodig. Indien jouw leverancier jouw Chromebooks nog niet onder centraal beheer gebracht heeft, doe je het volgende.

Bij opstart van een nieuwe Chromebook of een Chromebook waar een powerwash (factory reset) op uitgevoerd is, klik je na het verbinden met wifi en het accepteren van de voorwaarden op “Aanmelden voor Enterprise”. Hier voer je de inloggegevens in van een gebruiker met inschrijfrechten. Het Chromebook wordt nu geregistreerd in jouw Workspace omgeving voor centraal beheer.

Vanuit de beheeromgeving van Google Workspace kun je deze Chromebook nu in de gewenste organisatie-eenheid, zoals de klas, plaatsen.

4.3 Chromebook beheerde gastsessie

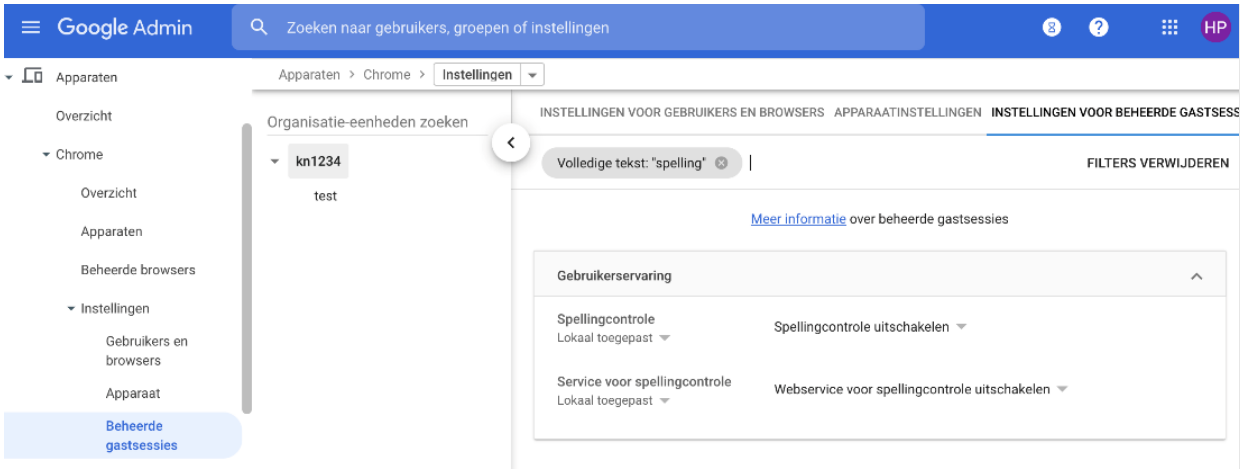
In een beheerde gastsessie start de gebruiker het Chromebook besturingssysteem op als gast in plaats van als gebruiker. De instellingen voor o.a. netwerk- en printerbeheer van het apparaat worden wel centraal door de ict-beheerder beheerd. De opslag van bestanden op het apparaat is van tijdelijke aard. Als je bijvoorbeeld een plaatje downloadt, dan wordt deze automatisch verwijderd bij het afsluiten van de Chromebook. Daarnaast opent gedurende een beheerde gastsessie de Chromebrowser ook altijd in gastmodus. Alle browsergerelateerde data (formulieren, browsergeschiedenis, cookies en inlogsessies op websites en webapplicaties) zijn tijdelijk en worden bij afsluiten van het apparaat verwijderd.

Bij het onder beheer plaatsen van een Chromebook, kun je ervoor kiezen om een Chromebook zonder gebruikersaccounts te gebruiken. Dit doe je door het Chromebook automatisch te laten opstarten in een beheerde gastsessie. In de Workspace Admin Console doe je dit onder Apparaten > Chrome > Instellingen > Instellingen voor beheerde gastsessies > Beheerde gastsessie automatisch starten.

In deze handleiding staan instellingen die voor gebruikers en browsers gelden. Deze zijn in te stellen via Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers. Als je Chromebooks in beheerde gastsessie binnen jouw organisatie gebruikt dan moet je al deze instellingen ook uitvoeren voor de gastsessies onder Apparaten > Chrome > Instellingen > Instellingen voor beheerde gastsessies.

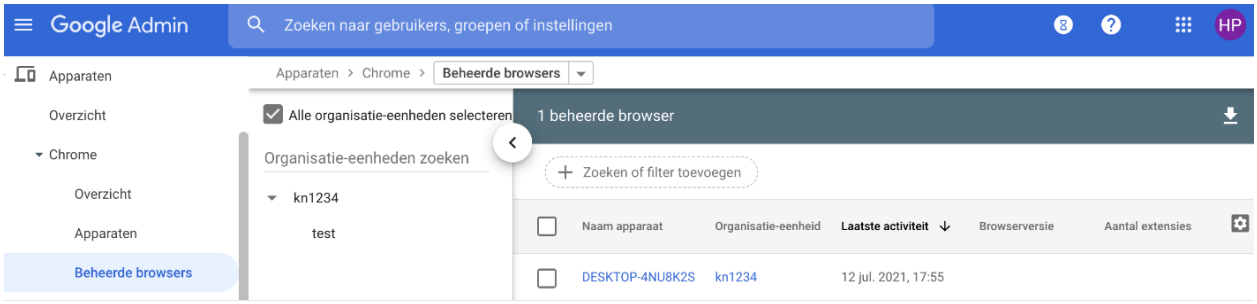
Als voorbeeld hieronder de instellingen voor spellingcontrole. Alle instellingen beschreven voor gebruikers en browsers moet je dus ook voor beheerde gastsessie uitvoeren.

Voorbeeld: Webservice voor spellingcontrole uitzetten voor beheerde gastsessies onder: Apparaten > Chrome > Instellingen > Instellingen voor beheerde gastsessies.



4.4 Chromebrowsers onder beheer brengen

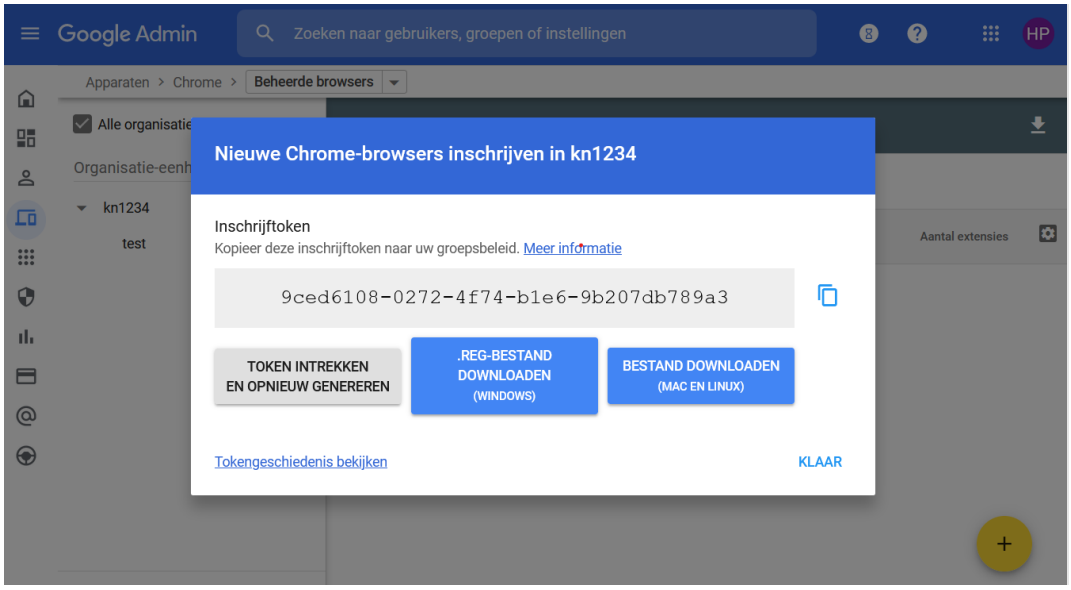
Je kunt de Chromebrowser instellingen alleen centraal beheren als deze onder beheer staan. Dit is te controleren in de Admin console onder Apparaten > Chrome > Beheerde browsers



Als je een ander besturingssysteem gebruikt, zoals Windows of Mac, dan voer je de volgende stappen uit:

1. Token voor beheer genereren vanuit de Admin Console.
2. Beheerderspolicy met de beheerderstoken instellen op uw besturingssysteem.

Je genereert de token onder Apparaten > Chrome > Beheerde browsers. Rechtsonder in beeld klik je op het gele plusteken (‘+’).



De token installeer je volgens het groepsbeleid van jouw besturingssysteem via het beleid ‘CloudManagementEnrollmentToken’. Hieronder lees je meer over groepsbeleid.

4.5 Instellingen op het besturingssysteem via groepsbeleid

Sommige van de te nemen maatregelen kun je direct op het besturingssysteem bewerkstelligen via een zogenaamde ‘group policy’, ofwel groepsbeleid. De instelling van het besturingssysteem hebben voorrang over de instellingen die via de Admin console zijn ingesteld. In de overzichtstabel van de maatregelen is terug te vinden welke policies je op welke manier kunt instellen via het groepsbeleid.

Als beheerder zul je of jouw leverancier voor het beheren van groepsbeleid gebruik maken van een zogenaamde Group Policy beheertool. Het algemene beheer van de apparaten van jouw organisatie valt buiten het bestek van deze handleiding. Hiervoor kun je eventueel terecht bij jouw leverancier.

Meer informatie over de instellingen via het besturingssysteem vind je op de pagina Lijst met Chrome Enterprise-beleid.

5 Instellingen in de Admin console

Maatregelen die de gebruiker en bijbehorende gebruikersaccounts betreffen, kunnen veelal centraal via de Google Workspace omgeving in de Admin console ingesteld worden. Je kunt deze beheerdersomgeving bereiken via admin.google.com.

5.1 Google Workspace als K-12 instellen

Het verplichte onderwijs in de Verenigde Staten beslaat dertien jaar. Het begint met een jaar kindergarten, een soort kleuterschool, gevolgd door 12 jaar klassikaal onderwijs, van de eerste tot en met de twaalfde klas. Daarom wordt dit systeem wel K-through-12 of K-12 genoemd. K-12 komt grofweg overeen met primair en voortgezet onderwijs in Nederland.

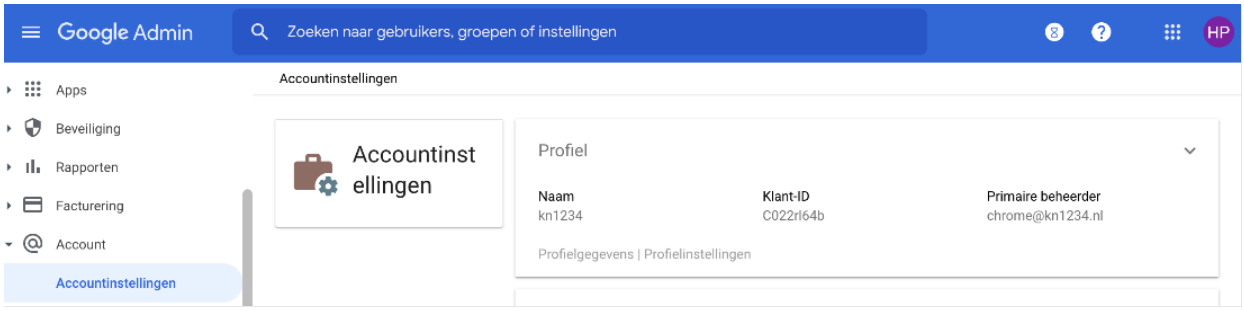
Om de privacy van kinderen op deze 'K-12 scholen' te beschermen kent Google Workspace for Education een speciale K-12 instelling. Met deze instelling staan alle personalisatie instellingen uit. Google Workspace als K-12 school gebruiken geeft de hoogte bescherming van persoonsgegevens. Ook voor onderwijsinstellingen in andere sectoren dan het po en vo bestaat de mogelijkheid om zelf te kiezen om deze K-12 instellingen in te stellen. Google zal hier niet op controleren of de onderwijsinstellingen een K-12 instelling is, of vrijwillig kiest deze instellingen toe passen op de eigen organisatie. Het kiezen voor deze instelling betekent de keuze voor *privacy by default*: één van de eisen van de AVG.

Als je kiest voor de optie K12, worden verschillende instellingen automatisch doorgevoerd waarbij de privacy van gebruikers standaard (beter) is beschermd. De standaard maatregelen zijn:

- Persoonlijke advertenties staan uit
- Toegang tot additionele diensten staat uit
- Toegang tot de Google marktplaats staan uit

Als de hele organisatie het kenmerk K12 krijgt, staan veel functies uit die je wellicht wel wilt toestaan voor leraren. Het is daarom niet nodig de hele organisatie op K12 te zetten. Dit kan per organisatie-eenheid. Bijvoorbeeld 1 organisatie-eenheid voor leerlingen en 1 voor leraren. Meer informatie hierover vind je op deze pagina.

In de Admin console van Google Workspace selecteer je organisatietype Primary/secundairy education onder: Accountinstellingen > Profiel > organisatietype.



5.2 Gebruikersnamen in email adres

Het is aan te bevelen om niet de naam van medewerkers, leerlingen of studenten te gebruiken in het emailadres. Maak e-mailadressen anoniem of in ieder geval minder herleidbaar. Bijvoorbeeld door het unieke leerlingnummer of personeelsnummer in het e-mailadres te gebruiken in plaats van de naam. Dus leerling123@school.nl in plaats van jan.jansen@school.nl. Deze maatregel zorgt ervoor dat de privacy van de leerling beter is beschermd, omdat uit het e-mailadres geen persoon is af te leiden.

Waarom deze maatregel? Een voorbeeld: je hebt allemaal wel eens een mail ontvangen voor een bijeenkomst met een enorme lijst aan mensen zichtbaar in de cc. Dit is feitelijk een datalek. Door in ieder geval bij kinderen anonieme mailadressen te gebruiken voorkom je dit soort lekken.

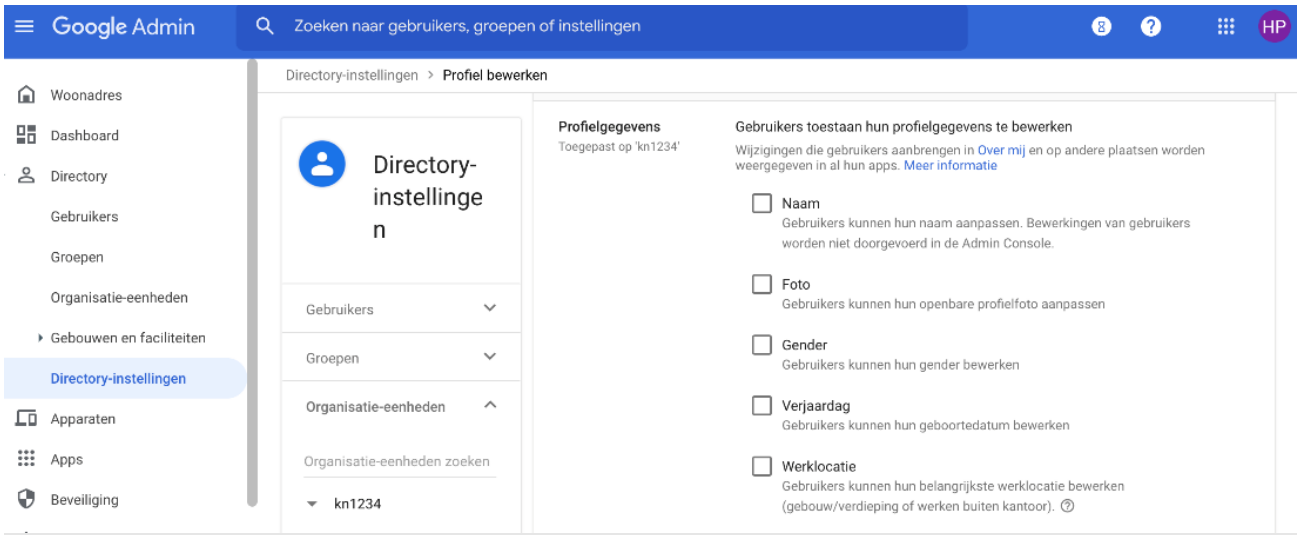
Doordat het e-mailadres en leerlingnummer in de directory zijn gekoppeld aan andere gegevens van de leerling, blijft de leerling binnen de organisatie identificeerbaar en ook voor Google. De voornaam en achternaam staan dus wel in de directory, maar niet in het emailadres. Als je een e-mail van leerling123@school.nl ontvangt, toont Google Mail dus de naam van de leerling bij dit e-mailadres. Maar als het e-mailadres gelekt wordt (buiten de Google-omgeving), wordt de naam van de leerling niet bekend.

Let op: als het e-mailadres als unieke identifier gebruikt wordt voor single-sign-on bij andere systemen is de overstap naar een anoniem e-mailadres lastiger. Je kunt er dan voor kiezen om de bestaande accounts te behouden zoals ze zijn en de nieuwe accounts anoniem te maken. Je beschrijft deze aanpak in de lokale DPIA. Ook het beheeraccount kan een fictieve naam hebben. Dit staat beschreven in de [Workspace for Education Data Protection Implementation Guide.]

5.3 Gebruikersprofielen

Beheerders kunnen instellen dat gebruikers hun profiel niet kunnen aanpassen. Hierdoor voorkom je dat medewerkers, leerlingen of studenten alsnog persoonlijke data toevoegen en hun profiel aanvullen met gevoelige gegevens.

Instellen onder: Directory instellingen > Profiel bewerken.



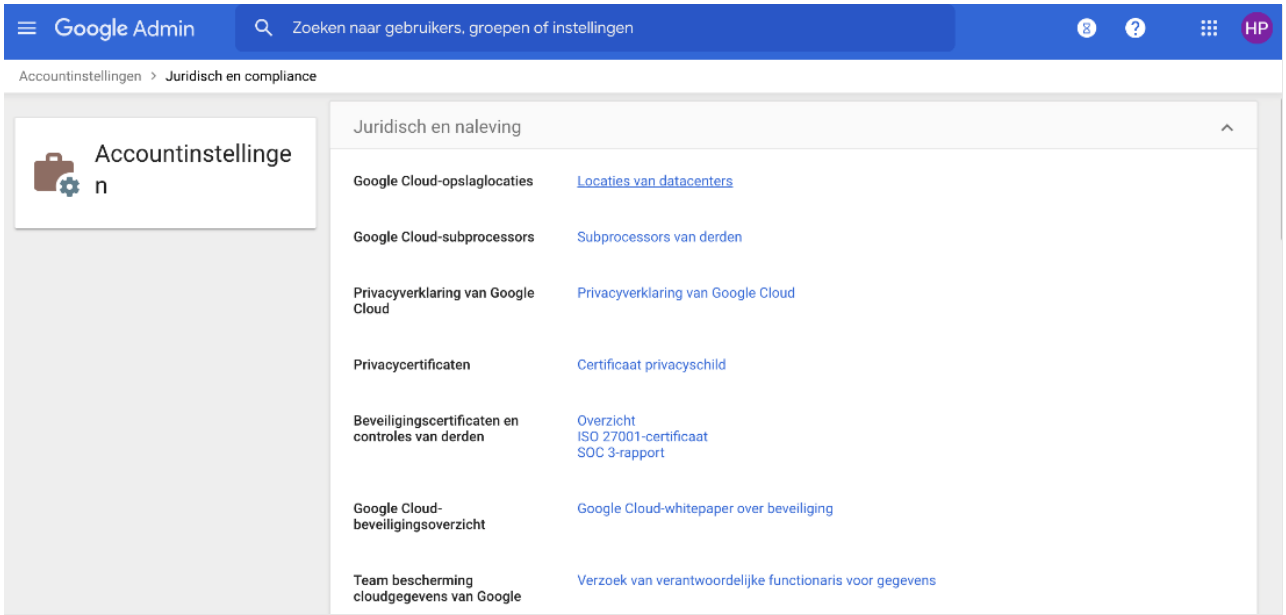
5.4 Geografische locatie dataopslag

Als beheerder kunt u bepaalde gegevens opslaan in een specifieke geografische locatie door een beleid voor gegevensregio's te gebruiken. De opties voor geografische locaties zijn de Verenigde Staten en Europa.

Dataopslag in Europe geef je de hoogste bescherming van persoonsgegevens. Om Europa als dataopslag te kunnen instellen, heb je de versie Educations standard of plus van Workspace for Education nodig.

De optie om gegevens binnen Europa op te slaan is alleen opgenomen in de betaalde versies van Google Workspace for Education. Het opslaan van gegevens binnen Europa is een van de maatregelen die genomen kunnen worden om het privacyrisico van gegevensuitwisseling met de Verenigde Staten te beperken. In de Update DPIA Report van 2 augustus 2021 [https://sivon.nl/wp-content/uploads/2022/07/Update-DPIA-report-Google-Workspace-for-Education-2-augustus-2021.pdf] staat 'data storage in the EU where possible'. Kies dus voor opslag binnen Europa als dat (technisch) mogelijk is. SIVON werkt nog aan een data transfer impact assesment (DTIA). Deze is in juli 2024 afgerond en te vinden op de SIVON website.

Instellen onder > Admin console > Account instellingen > Juridisch en Compliance.



5.5 Aanvullende Google diensten (Additional Services)

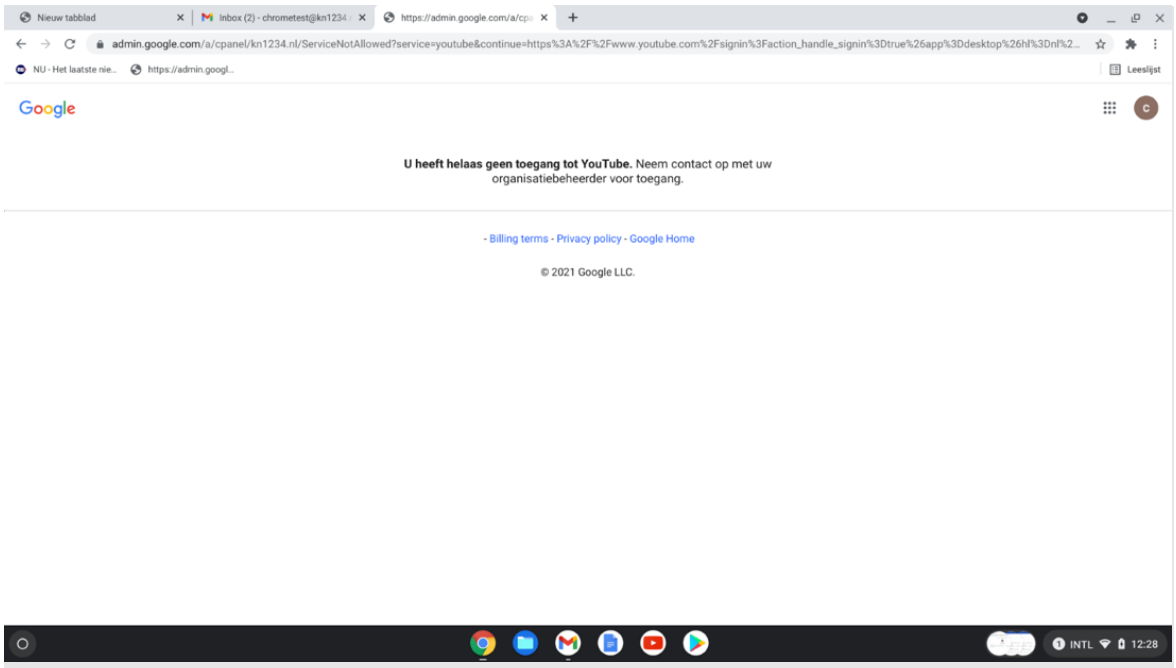
Aanvullende Google diensten vallen niet onder de Google Workspace overeenkomst die SURF en SIVON met Google hebben afgesloten. Deze aanvullende diensten moeten dus uitstaan.

Door het gebruik van deze Additional Services zouden onderwijsinstellingen Google toegang geven tot informatie van hun medewerkers, leerlingen of studenten, zonder dat de onderwijsinstellingen de volledige controle houden over hun gegevens. Dat zou in strijd zijn met de AVG. Dat betekent dat toegang tot aanvullende services (standaard) uitgeschakeld moet zijn.

- Wanneer de toegang tot Aanvullende diensten is geblokkeerd, kunnen medewerkers, leerlingen of studenten wel Google Search nog steeds gebruiken omdat automatisch uitloggen in SafeSearch-modus aanstaat. Hierdoor worden zij niet gevolgd door Google omdat zij 'onzichtbaar' worden uitgelogd, zodat Google de gebruiker van Zoeken niet kent. Een privacyvriendelijke zoekmachine gebruiken is ook mogelijk zoals bijvoorbeeld Duck-Duck-Go.
- Het gebruik van YouTube door medewerkers, leerlingen of studenten is niet mogelijk zolang zij ingelogd zijn in hun account van Workspace for Education. Leraren kunnen alleen gebruik maken van YouTube-video's door deze te embedden in privacy enhanced mode, bijvoorbeeld door de (link naar de) video op te nemen in Classroom of Slides. Hierdoor kunnen video's nog wel bekeken worden.
- Studenten in het mbo en ho die er zelf voor kiezen om Scholar, YouTube of andere aanvullende services te gebruiken, moeten zich afzonderlijk bij Google aanmelden voor een consumentenaccount. Zij moeten uitloggen uit hun account van Workspace for Education bij de onderwijsinstelling. Google, en niet de universiteit, is dan verantwoordelijk voor het verkrijgen van geldige toestemming van deze studenten (van 16 jaar en ouder) voor de gegevensverwerking in dergelijke privé Google-accounts.

YouTube

Doordat aanvullende Google-diensten niet onder de Google Workspace for education-overeenkomst vallen, moeten deze diensten **uit** staan. YouTube is een van de aanvullende diensten. Het gebruik ervan is een hoog risico voor medewerkers, leerlingen of studenten, omdat de school geen controle heeft over hun persoonsgegevens die Google verzamelt of gebruikt.
Je kunt door het uitzetten van de aanvullende diensten niet meer inloggen bij YouTube met jouw Google Workspace-account. Dit betekent dat je geen playlists meer kunt aanmaken of video's kunt uploaden. Je kunt wel nog video's bekijken in de embedded mode, zoals beschreven in de technische handleiding. Als je de YouTube player embed in Workspace core service (zoals sites of classroom), worden er geen advertenties meer getoond. De YouTube-cookies van de embedded player voldoen aan de nieuwe privacyvoorwaarden.

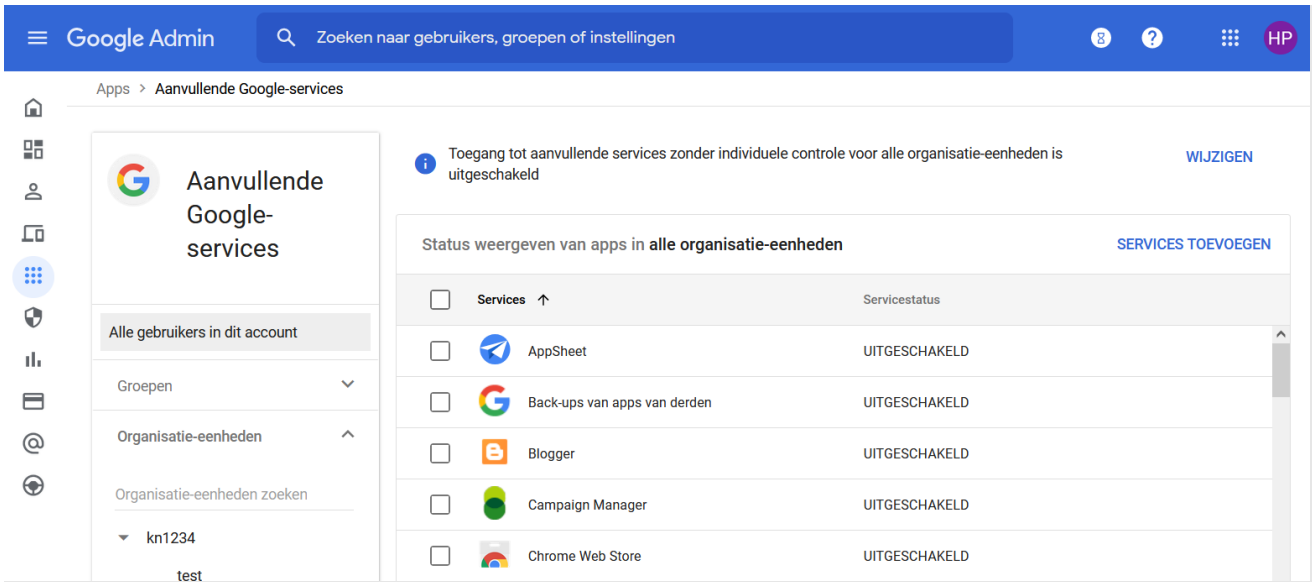


Youtube workaround:

- Je kunt in Google Workspace een organisatie-eenheid creëren waarin afgeweken wordt van de geldende privacy-instellingen. In deze organisatie-eenheid kun je enkele generieke, anonieme accounts aanmaken die wel toegang krijgen tot YouTube. Als deze accounts niet tot personen te herleiden zijn, bijvoorbeeld youtubebeheer1@school.nl, heeft dit geen of weinig impact op de privacy. Vanaf deze accounts kun je dan toch video's uploaden.
- Ook zijn er scholen die gebruikmaken van een laptop of computer waarop niet of anoniem is ingelogd. Leerlingen kunnen in de klas dan op die laptop of computer YouTube gebruiken voor huiswerkopdrachten. Op deze manier worden ook geen persoonsgegevens verzamelt, waardoor er geen (hoog) privacyrisico is.
- Bij zoeken naar video's in duck duck go, kan de video embedded in de zoekresultaten weergegeven worden zonder naar www.youtube.com te gaan.
- Let op: zorg er in alle gevallen voor dat er geen audiovisueel materiaal van herkenbare kinderen wordt geüpload. Google is daarvoor nog steeds verwerkingsverantwoordelijke.

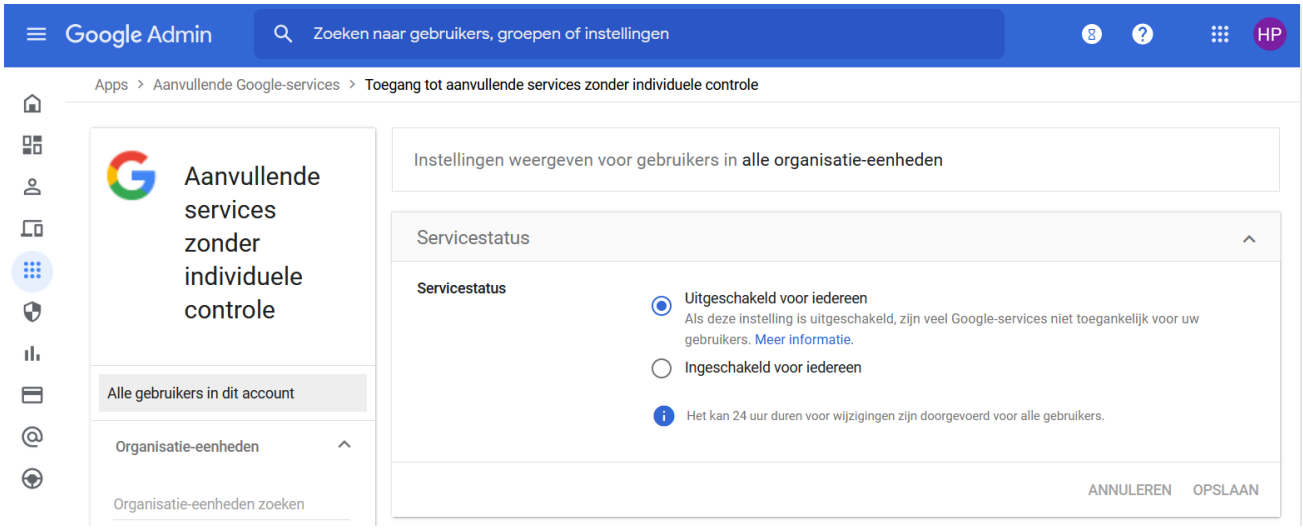
Aanvullende services kunnen individueel aan- of uitgezet worden.

Instellen onder: Admin console > Apps > Aanvullende Google services > Uitschakelen voor iedereen.



De instelling kan ook generiek voor de hele organisatie.

Instellen onder: Apps > Aanvullende Google services> Toegang tot aanvullende services zonder individuele controle > Uitgeschakeld voor iedereen.

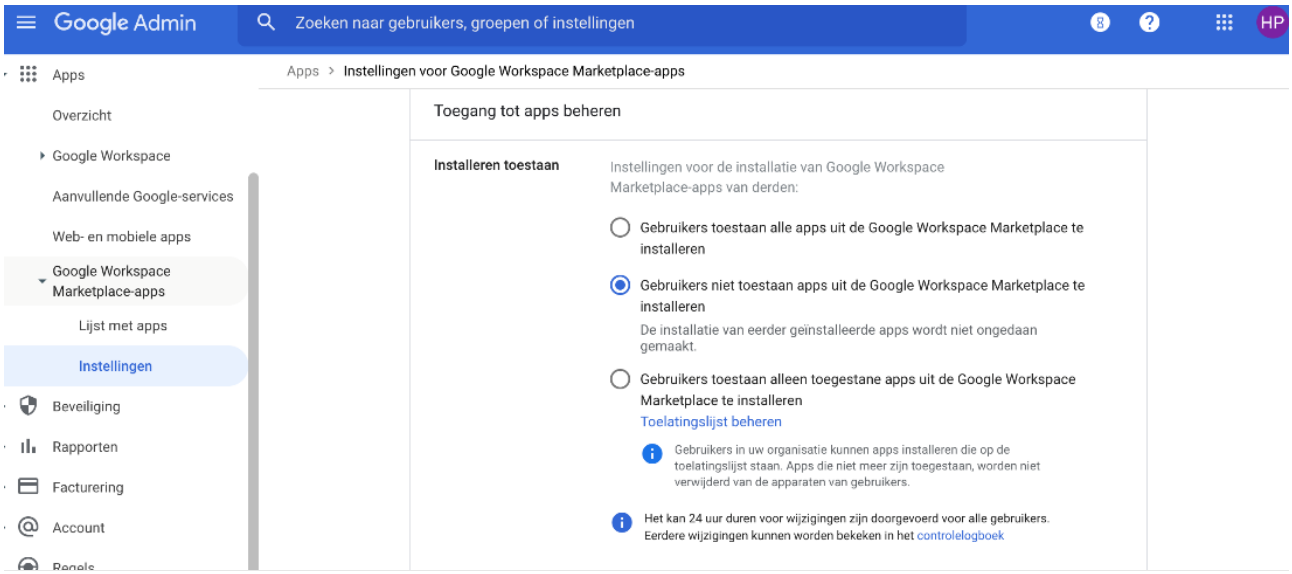


Er zitten privacy risico's aan het gebruik van YouTube ook als je YouTube vanuit een Microsoft omgeving gebruikt legt Google jouw gedrag vast. Toch YouTube gebruiken? Realiseer je dan dat kinderen advertenties te zien krijgen, u geen controle heeft over wat kinderen te zien krijgen. Om het volgen van gebruikers te voorkomen kunt u embedded mode zoals hierboven beschreven gebruiken of op een anoniem shared device.

5.6 Google Workspace Marketplace-apps

Het gebruik van allerlei (niet-geverifieerde) Marketplace-apps leidt tot privacyrisico's. Als medewerkers, leerlingen of studenten vanuit het Workspace for Education account dergelijke apps aanschaffen of downloaden, wordt de school daar verantwoordelijk voor. Dat is niet wenselijk omdat de onderwijsinstelling de controle kwijt is over de gegevens die naar (al) deze leveranciers toegaan. Daarom wordt deze optie uitgezet, en kunnen medewerkers, leerlingen en studenten alleen Marketplace-apps gebruiken die vooraf door de onderwijsinstelling zijn goedgekeurd.

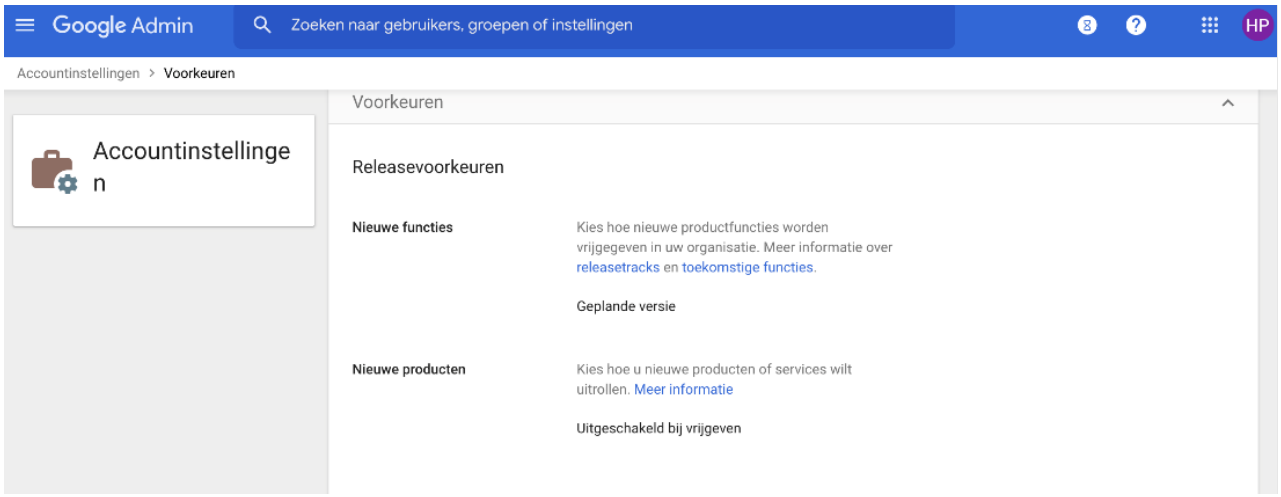
Instellen onder: Admin console > Apps > Instellingen voor Google Workspace Marketplace-apps > Gebruikers niet toestaan apps uit de Google Workspace Marketplace te installeren.



5.7 Nieuwe Google producten

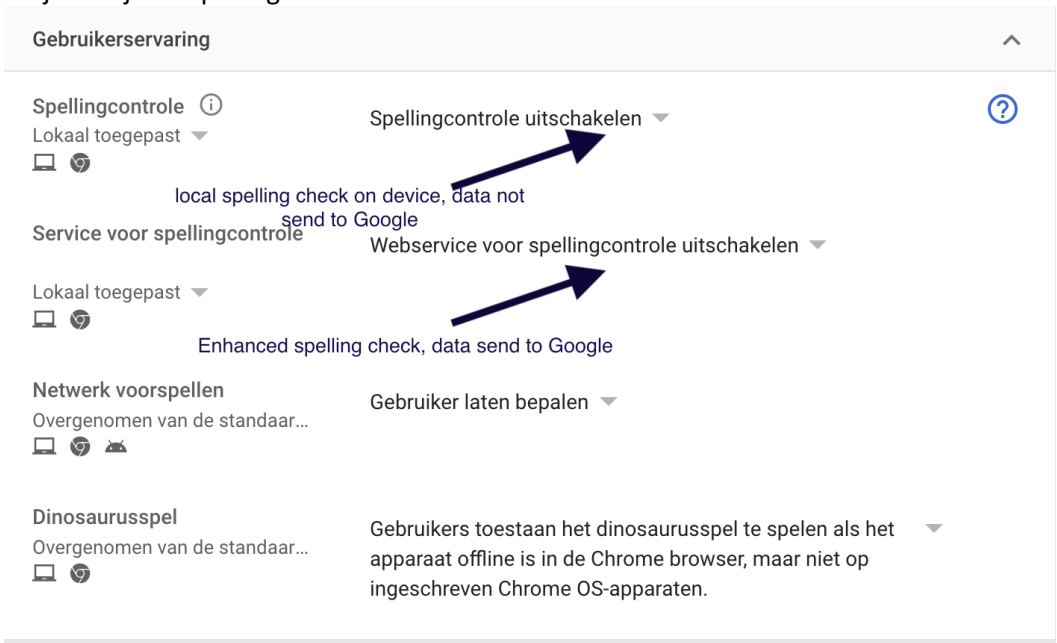
Beheerders kunnen privacyrisico's vermijden door nieuwe producten niet automatisch beschikbaar te stellen voor gebruikers. Nieuwe diensten kunnen dan eerst aan een analyse én DPIA onderworpen worden voordat ze beschikbaar gemaakt worden.

Instellen onder: Admin console > Accountinstellingen > Voorkeuren > Nieuwe producten > Uitschakelen bij vrijgeven.



5.8 Spellingcontrole en Spellingcontrole Webservice

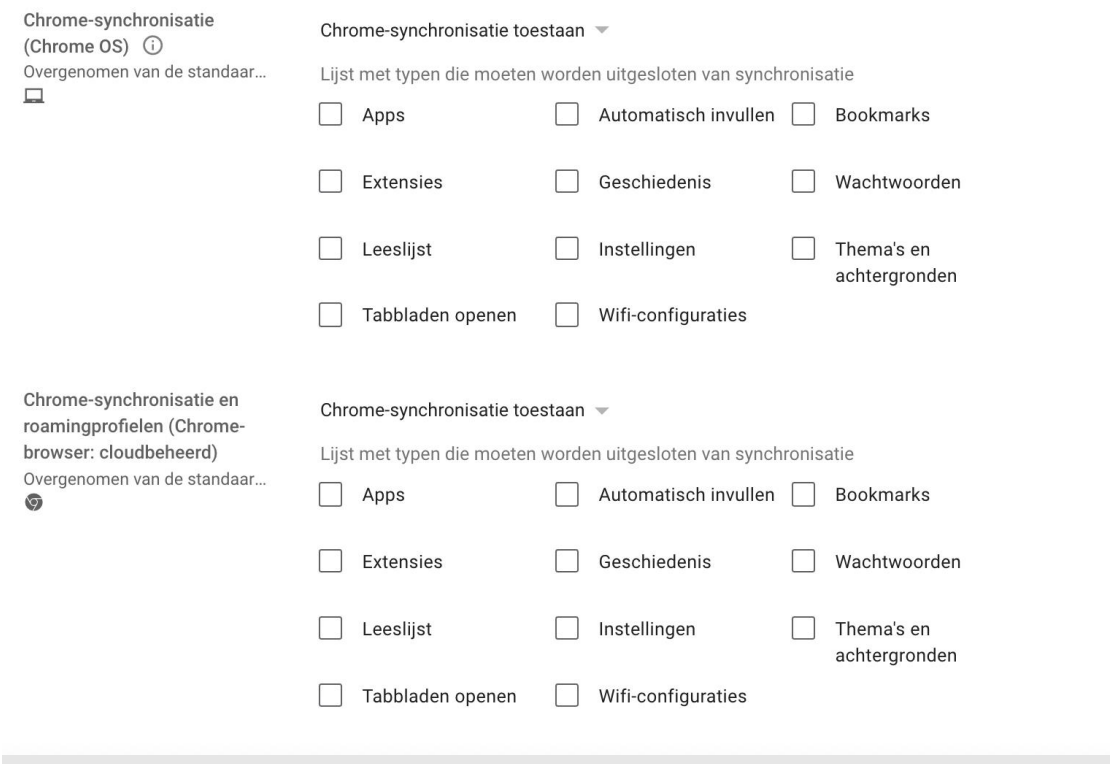
Er zijn 2 typen spellingcontroles. De 'gewone' lokaal op het device en de 'enhanced' die werkt met w ebservice. Bij de enhanced-versie gaat alle data waar u een spellingcontrole op uitvoert naar Google. Deze optie moet daarom uitstaan. De lokale spellingcontrole kun je aan laten staan. In de screenshot zie je hoe je de spellingcontrole uitschakelt.

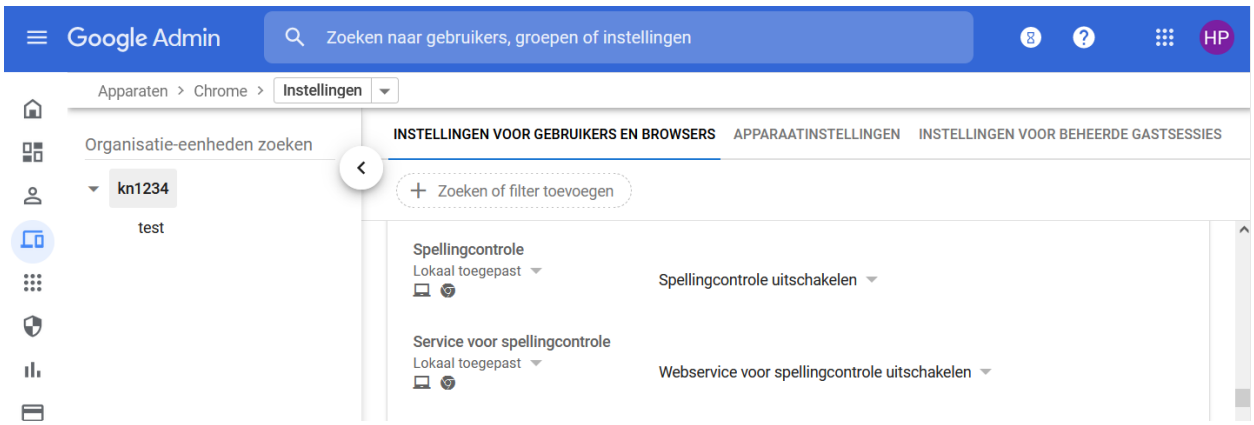


Instellen onder: Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers > Gebruikerservaring > Spellingcontrole > webservices voor spellingscontrole uitschakelen.

5.9 Chrome synchronisatie uitschakelen

Het doel van deze setting is om synchronisatie van o.a. favorieten met Google en daarmee samenhangende privacyrisico's te beperken.
Synchronisatie van gegevens kan voorkomen worden door instelling onder: Apparaten > instellingen voor gebruikers en browsers > andere instellingen
In de DPIA op Chrome OS en Chrome browser staat het advies om synchronisatie uit te zetten.



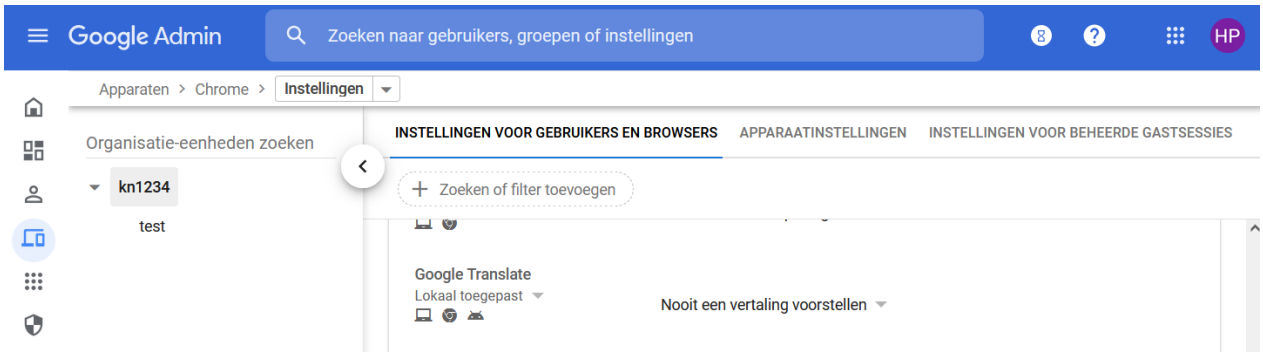


Meer informatie vind je in de Google Chrome Spelling Privacy Whitepaper.
https://www.google.com/intl/en/chrome/privacy/whitepaper.html#spelling

5.10 Automatische vertaling websites uitzetten

Wat geldt voor het uitzetten van de spellingscontrole, geldt ook voor de vertaalfunctie van Google voor websites die worden bezocht. Deze werkt uiteraard alleen als de data door Google verwerkt kan worden. Om de data niet te delen moet deze functionaliteit uitstaan.

Instellen onder: Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browser > Gebruikerservaring > Nooit een vertaling voorstellen.

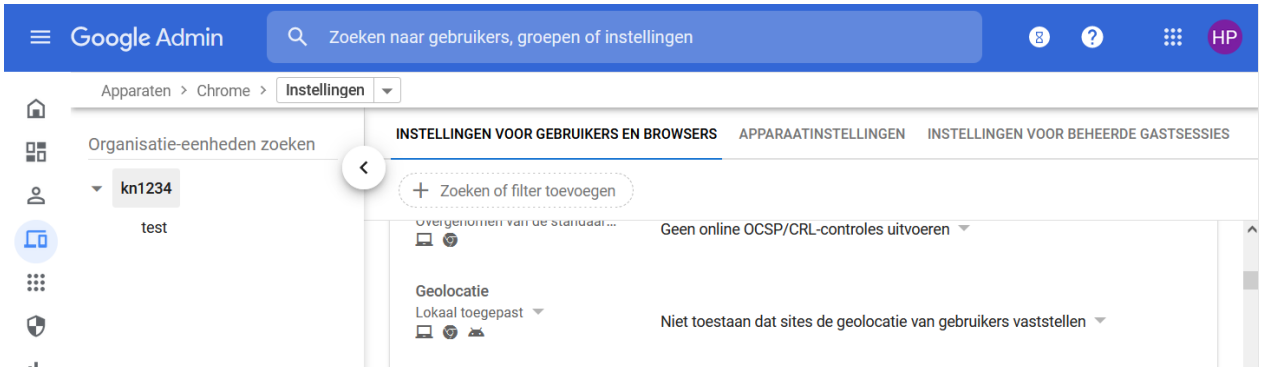


Meer informatie vind je in de [Google Chrome Privacy Whitepaper in de paragraaf Translate].

5.11 Geolocatie uitzetten

De geolocatie functie stelt websites in staat om op basis van IP-adres de locatie van de gebruiker te bepalen. Door dit uit te zetten, weet Google niet (standaard) waar de gebruiker zich bevindt en wordt het aantal verwerkte persoonsgegevens beperkt. Deze functie moet daarom uitgezet worden.

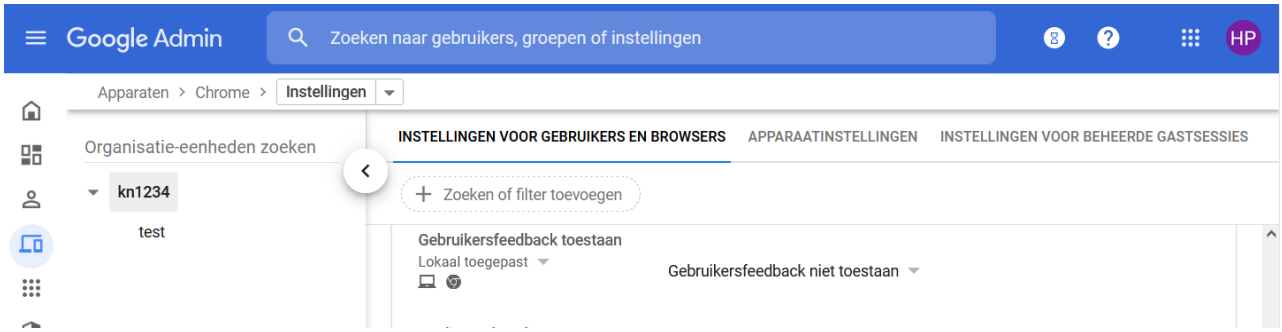
Instellen onder: Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers > Geolocatie > Niet toestaan dat sites de geolocatie van gebruikers vaststellen.



5.12 Gebruikersfeedback niet toestaan

Gebruikers niet toestaan dat ze feedback delen met Google. Als je het beleid niet instelt, kunnen gebruikers feedback naar Google sturen. Hierbij kan veel persoonlijke of zelfs gevoelige informatie worden gedeeld waar Google (en niet de onderwijsinstelling) verantwoordelijk voor is.

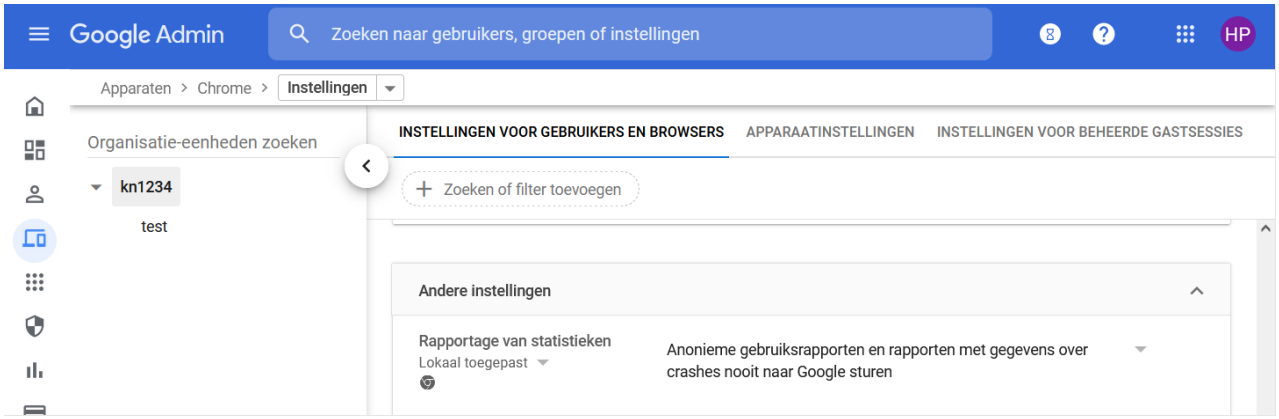
Instellen onder: Apparaten > Chrome > Instellingen voor gebruikers en browsers > Gebruikerservaring > Gebruikersfeedback Toestaan > Gebruikersfeedback niet toestaan.



5.13 Rapportage van statistieken: turn off

Voor het maken van gebruiksstatistieken en –rapportages, verzamelt Google gegevens. Door dit uit te zetten, wordt het aantal persoonsgegevens dat Google gebruikt, beperkt. Daarmee worden privacyrisico's beperkt.

Instellen onder: Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers > andere instellingen > Rapportage van statistieken > Anonieme gebruikersrapporten en rapporten met gegevens over crashes nooit naar Google sturen.

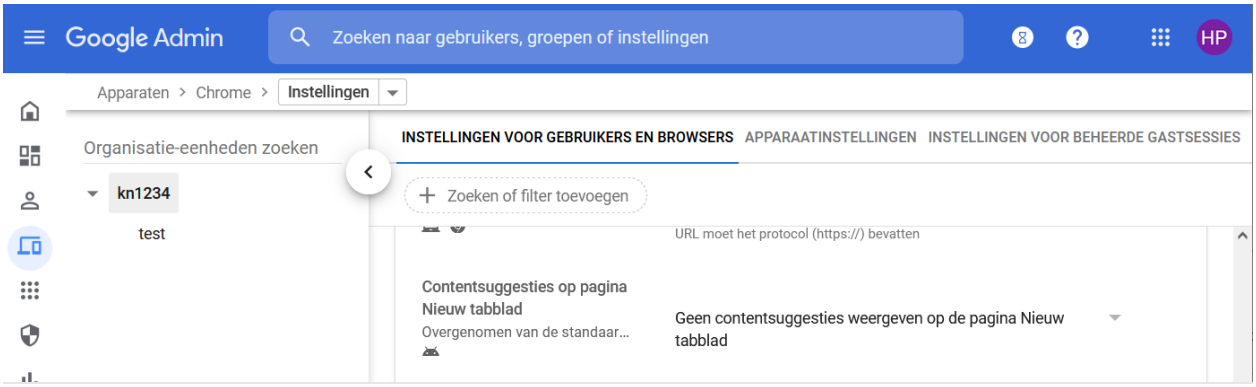


5.14 Nieuw Tabblad

Bij een nieuw tabblad kan Google helpen met het doen van suggesties. Hiervoor houdt Google informatie bij over welke websites de gebruiker bezoekt. Dat is niet wenselijk want het aantal verwerkte persoonsgegevens moet zo beperkt mogelijk zijn. Daarom moet deze instelling worden uitgezet.

In de Admin console zijn drie plekken onder Apparaten > Chrome > Instellingen waar nieuw tabblad-beleid gewijzigd moet worden.

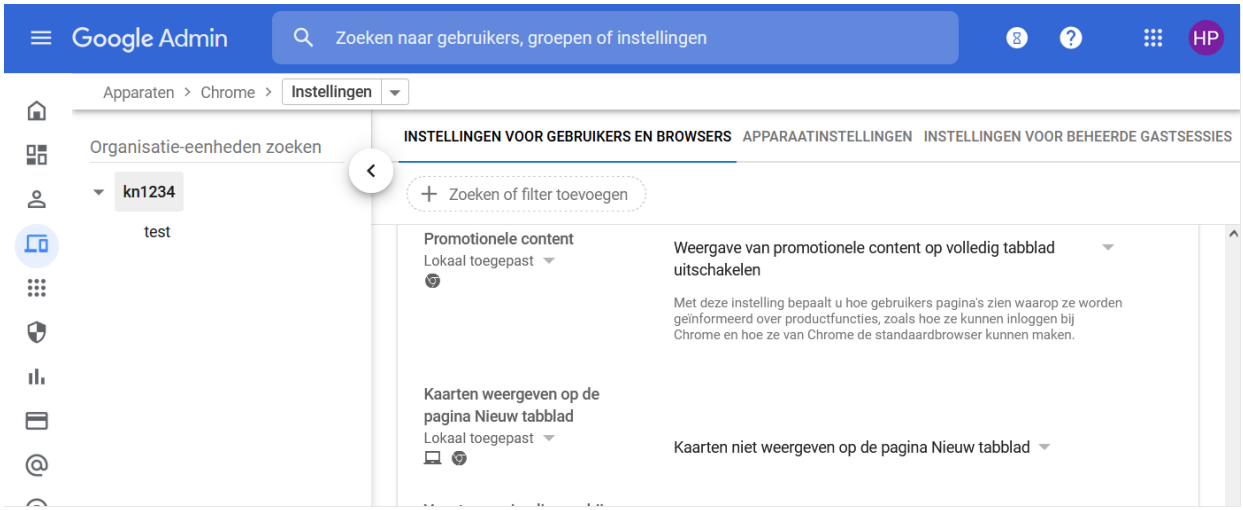
1) Apparaten > Chrome > instellingen voor gebruikers en browser > Geen contentsuggesties weergeven op pagina nieuw tabblad.



2) Apparaten > Chrome > Instellingen voor gebruikers en browser > Weergave promotionele content op volledig tabblad uitschakelen.

3) Apparaten > Chrome > Instellingen voor gebruikers en browser > Kaarten niet weergeven op de pagina nieuw tabblad.

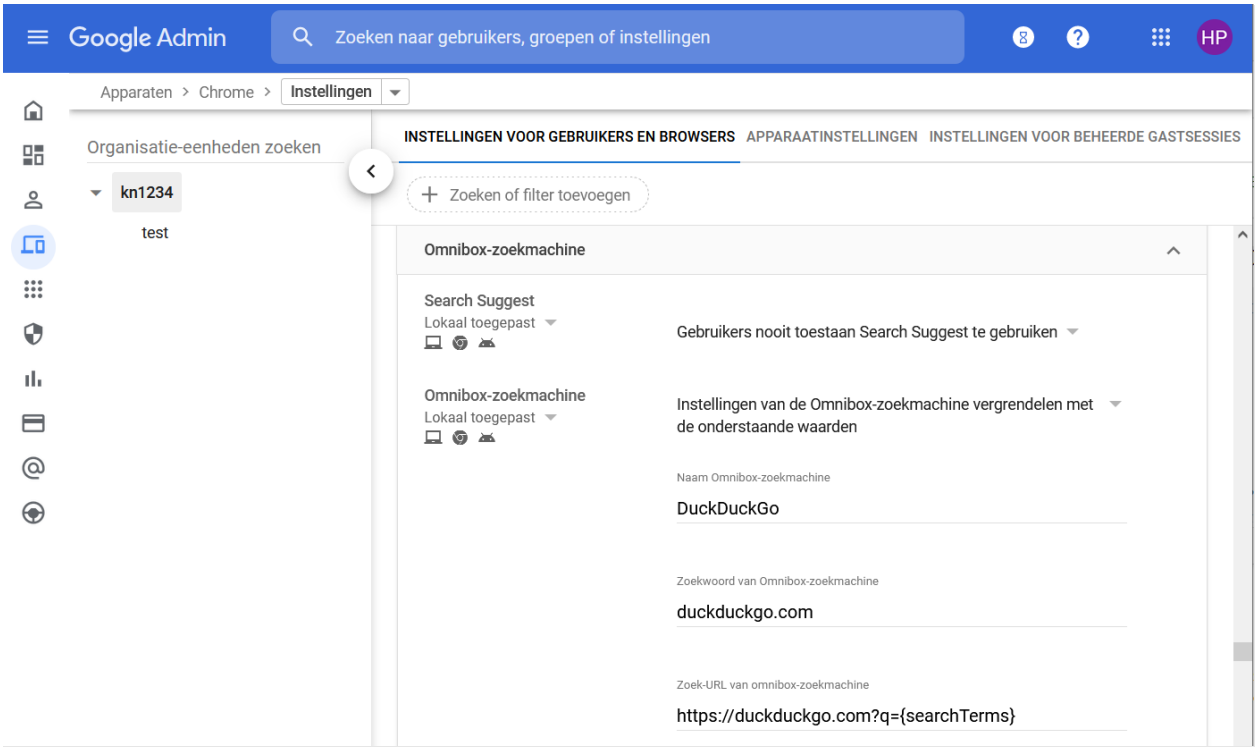
Kaarten zijn “buttons” in het nieuwe venster van veel bezochte websites of populaire websites geselecteerd door Google als er nog geen browser geschiedenis is.



5.15 Search suggested service (omnibox)

De functie *download search suggesties* wordt getoond aan ingelogde gebruikers bij het openen van een nieuw tabblad. Voor deze suggesties moet Google webbrowser historie bijhouden. Om het verzamelen en delen van deze persoonlijke data met Google te voorkomen moet deze functie uit staan.

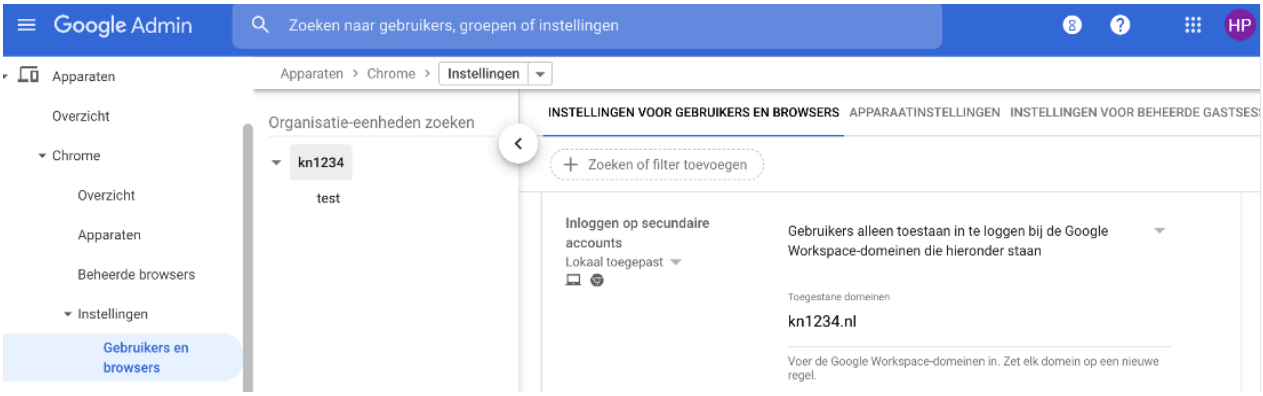
Instellen onder: Apparaten > Chrome> Instellingen> Instellingen voor gebruikers en browsers > Omnibox-zoekmachine > Gebruikers nooit toestaan search suggest te gebruiken



5.16 Inloggen op secundaire accounts

Om te voorkomen dat medewerkers, leerlingen of studenten hun privé Google-account koppelen aan het schoolaccount en daarmee alsnog worden blootgesteld aan privacyrisico's moet het inloggen op secundaire accounts verboden worden.

Instellen onder: Apparaten > Chrome > Instellingen voor gebruikers en browsers > Gebruikerservaring > Inloggen op secundaire accounts > Gebruikers alleen toestaan in te loggen op Workspace domeinen die hieronder staan (alleen schooldomein toevoegen).



5.17 Cookies beleid

Medewerkers, leerlingen of studenten klikken bij cookies op akkoord zonder zich goed te realiseren waarop ze akkoord geven. Daarom is het aan te bevelen bepaalde cookies te blokkeren.

Er zijn verschillende type cookies:

- **First party cookies** worden gemaakt door de website die je bezoekt. De site wordt weergegeven in de adresbalk.

- **Third party cookies** worden gemaakt door andere sites. Deze sites zijn eigenaar van een deel van de content (zoals advertenties of afbeeldingen) die je ziet (of niet ziet met bijvoorbeeld Facebook-pixels) op de webpagina die je bezoekt. Deze third party cookies kunnen functioneel, analytisch of tracking zijn. Een adverteerder kan met deze cookies een profiel opbouwen over uw surfgedrag. Hierdoor weet de third party dus meer van je dan de first party. Dit is een hoge vorm van inbreuk op de privacy.
- **Functionele cookies** zijn nodig om een website beter te laten functioneren. Dit zijn bijvoorbeeld bestanden die bijhouden wat er in een winkelwagentje zit.
- **Analytische cookies** worden gebruikt om onder andere bezoekersstatistieken bij te houden.
- **Tracking cookies** volgen de bezoeker tijdens het bezoek aan een website en eventueel ook daarna. Dit wordt onder andere gebruikt voor retargeting. Een voorbeeld hiervan is een advertenties die je steeds overal terugziet en die je dus 'volgt'.

Third party cookies uitzetten

Waarom werken sommige diensten niet meer als de third party cookies uitstaan?
In een leeromgeving worden verschillende applicaties gebruikt. Sommige applicaties hebben third party cookies nodig om goed te kunnen functioneren. Een voorbeeld is Google Drive. Als de third party cookies zijn geblokkeerd, kun je niets downloaden uit Google Drive. Google Drive valt onder de Google Workspace voor Education-voorwaarden. De Google Drive-cookies kun je dus accepteren. Het accepteren van third party cookies is echter een globale instelling. Wat betekent dat als je de Google Drive-cookies accepteert, je daarmee in een keer alle third party cookies accepteert. Een workaround is werken met whitelists. Je kunt een whitelist maken van websites waarvan je weet dat de third party cookies geen inbreuk op de privacy veroorzaken. In de screenshot zie je hoe je whitelists instelt via de Google Workspace admin console.

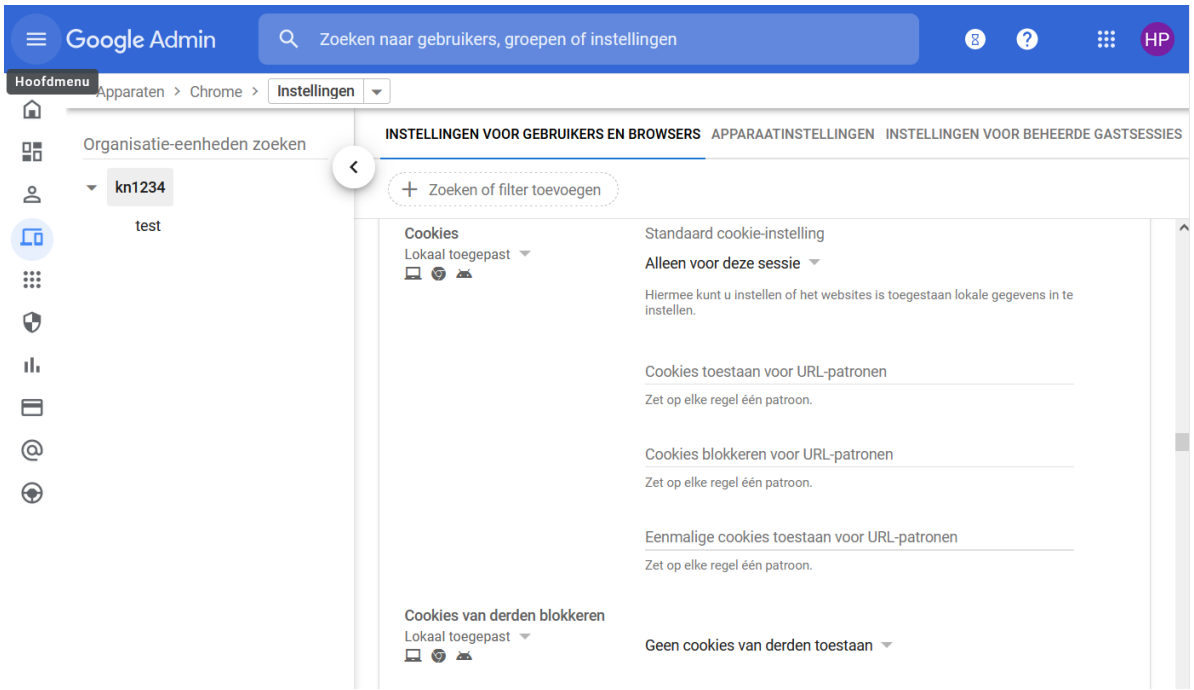
Cookies automatisch verwijderen?

Je kunt lokaal in de Chromebrowser instellen dat de cookies automatisch verwijderd worden als je de sessie sluit. Dit beperkt de impact van de tracking cookies. Je doet dit als volgt:

- Klik op de 3 puntjes rechtsboven > 'Instellingen'
- Kies 'Privacy en beveiliging' > 'Site-instellingen' > 'Cookies en andere sitegegevens'
- Kies voor de optie 'Cookies en sitegegevens wissen als je alle vensters sluit'

Je kunt dit ook centraal in Google Workspace instellen. Kies voor de cookiesinstelling 'Alleen voor deze sessie'. Dit heeft hetzelfde effect.
Bij deze maatregel staat het gebruik van (third party) cookies dus aan, maar worden deze cookies niet langer dan nodig opgeslagen. Als het blokkeren van third party cookies leidt tot grote problemen met het gebruik van verschillende webapplicaties, zijn er scholen die deze optie toepassen in combinatie met het (afgedwongen) gebruik van een adblocker.

Instellen onder: Apparaten > Chrome > Instellingen voor gebruikers en browsers > Content > Cookie & Cookies van derden.

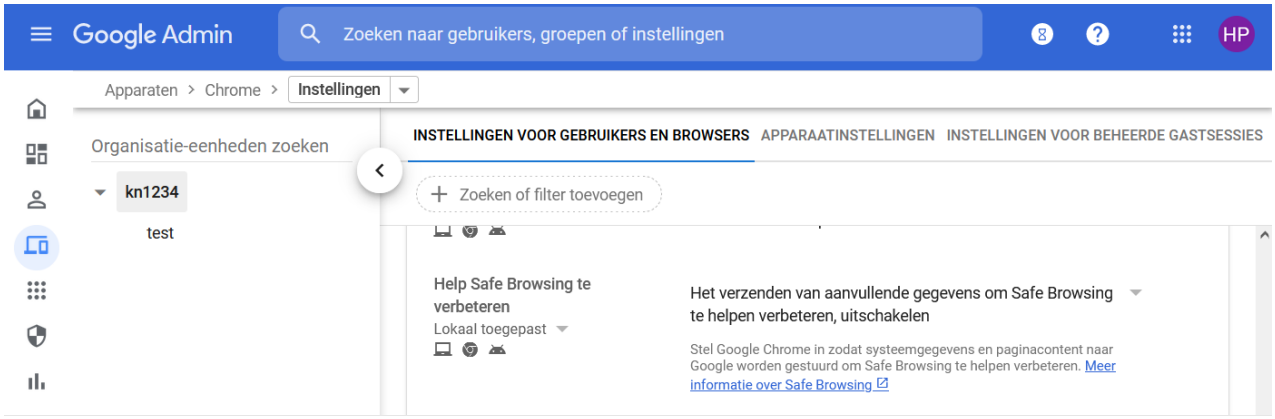


Als kinderen via de browser vrij toegang tot het internet hebben moeten cookies van derden eigenlijk altijd geblokkeerd worden. Simpelweg omdat je nooit weet wie die derden zijn en welke cookies ze plaatsen. In een gecontroleerde omgeving heb je afspraken met alle leveranciers over privacy inclusief de privacy van subverwerkers. Stel deze leverancier gebruikt embedded content van een subverwerker en deze subverwerker plaats derde cookies dan valt dat onder jouw overeenkomst. Neemt niet weg dat het geen kwaad zijn alert te zijn op ongewenste gevolgen.

5.18 Systeemrapportages van bezochte pagina's

Ten behoeve van de safe browsing functie stuurt de Chromebrowser regelmatig systeeminformatie en de inhoud van bezochte pagina's naar Google. De inhoud van dergelijke pagina's kunnen persoonsgegevens bevatten bij bijvoorbeeld het gebruik van leermiddelen. Het is niet nodig deze informatie bij te houden en te delen met Google. Zet deze systeemrapportages daarom uit.

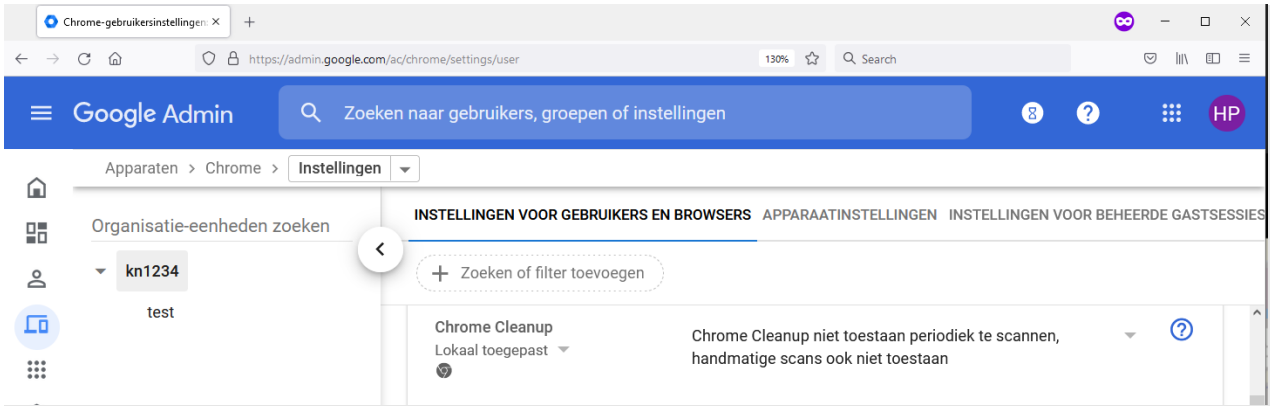
Instellen onder: Apparaten > Chrome > Instellingen voor gebruikers en browsers > andere instellingen > Help safe browsing te verbeteren > Het verzenden van aanvullende gegevens om safe browsing te helpen verbeteren uitschakelen.



5.19 Chrome Cleanup

Chrome Cleanup is een onderdeel van de Chromebrowser dat regelmatig de browser en systeemomgeving scant. Om de overdracht van gegevens te stoppen, moeten de resultaten van Chrome cleanup nooit met Google gedeeld worden.

Instellen onder: Apparaten > Chrome > Instlelingen voor gebruikers en browsers > Chrome cleanup > Resultaten van Chrome cleanup worden nooit gedeeld met Google.



6 Individuele instellingen en instructies

Slechts in een enkel geval zal een individuele gebruiker maatregelen hoeven nemen. In deze handleiding wordt zo veel mogelijk uitgegaan van gecentraliseerd beheer van de te treffen maatregelen.

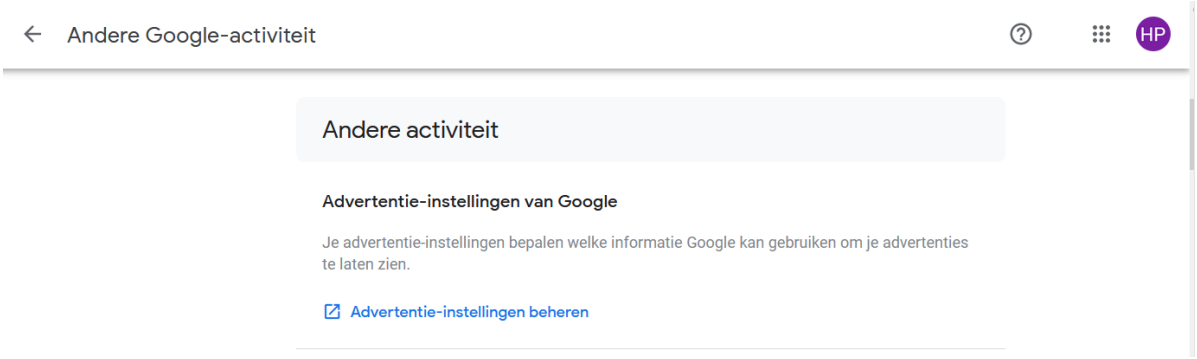
6.1 Advertentiepersonalisatie

Let op: deze maatregel is alleen van toepassing als het hierboven genoemde ‘K-12 profiel’ **niet** is ingesteld voor de gebruikersaccounts. Onderwijsinstellingen die niet gekozen hebben voor K-12, moeten de volgende instellingen dus zelf handmatig toepassen.

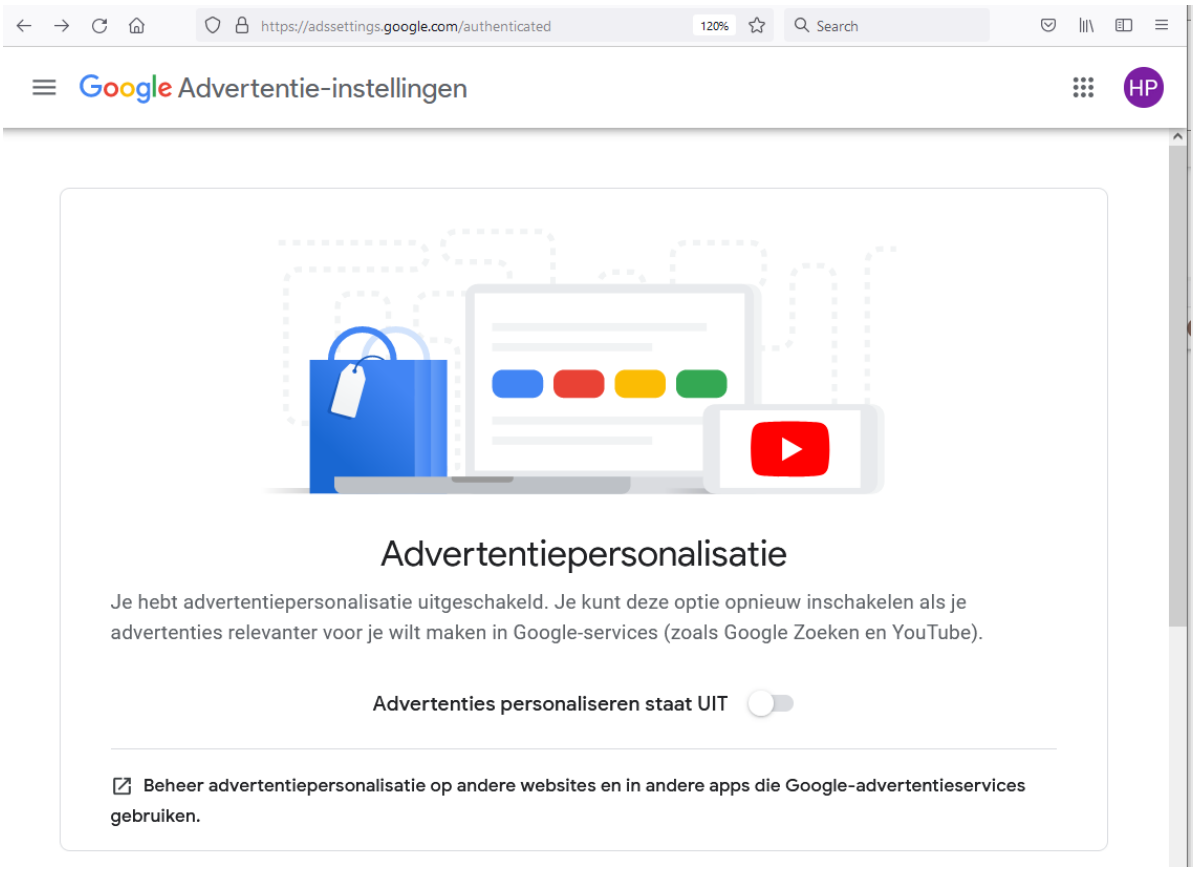
Advertenties die door Google op internetpagina's worden getoond aan een gebruiker worden gebaseerd op de persoonlijke informatie uit een Google-account, persoonlijke zoekopdrachten, browsegedrag en profilering aan de hand daarvan.

Advertentiepersonalisatie maakt gebruik van verscheidene persoonsgegevens die tijdens het browsen over internet worden verzameld. Om de data-overdracht en ontwikkeling van persoonsgegevens te onderbreken dient advertentiepersonalisatie uitgeschakeld te zijn.

Google zal bij nieuwe 'Education' accounts voor Workspace for Education deze personalisatie van advertenties uitzetten. Bestaande gebruikers moeten dit echter per gebruiker op hun eigen 'MyActivity' pagina wijzigen via myactivity.google.com.



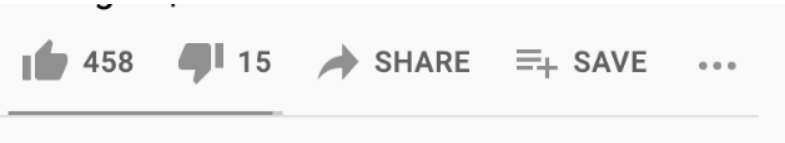
Ga via het menu naar 'Andere Google-activiteit' en klik op 'Advertentie-instellingen beheren'. Verschuif op deze pagina de knop naar 'Uit'.



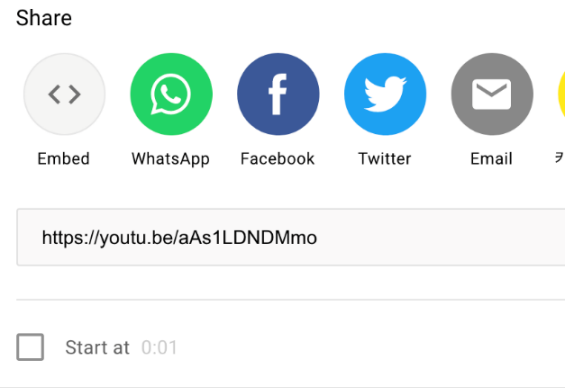
6.2 YouTube video embedding

Bij direct gebruik van de Aanvullende dienst YouTube ontvangt Google privacygevoelige tracking data. Het is aan te bevelen YouTube video's in embedded mode te gebruiken. In embedded mode worden er geen tracking cookies gebruikt. Hieronder staat beschreven hoe je dat doet.

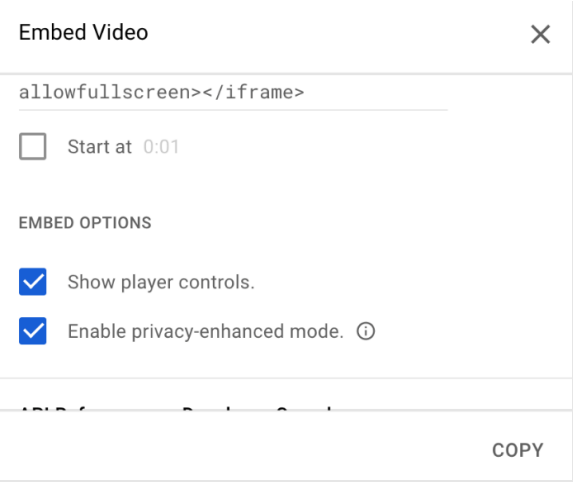
Onder elke YouTube video staat een share button



Klik hierop om op het volgende scherm te komen en selecteer "embed"



Vervolgens is het mogelijk een stukje code te kopiëren met 'enable privacy-enhanced mode'.



Deze code kunt je vervolgens publiceren op een website zoals Google sites. Vanaf daar kun je nu direct de YouTube video afspelen.

6.3 Gebruik van Chromebrowser

Er is een nieuwe versie van Chromebrowser beschikbaar gekomen op 18 augustus 2023 waarbij Google als data verwerker optreedt in plaats van data controller. Deze verwerker versie van Chromebrowser is alleen beschikbaar op Chromebooks. Voor PC's die geen Chrome OS gebruiken

(Windows, Mac, Linux) adviseren we alternatieve browsers zoals bijvoorbeeld Duck duck go, Mozilla, Firefox of Safari.

7 Gebruik Google niet als zoekmachine

In plaats van Google search adviseren we het gebruik van een privacyvriendelijk alternatief zoals DuckDuckGo of Startpage.

7.1 Gebruik een advertentie- en/of tracking blocker

Overweeg het gebruik van een advertentie- en/of tracking blocker. Advertenties op websites gebruiken tracking om browse gedrag te volgen.

Een adblocker (zoals uBlock Origin of Adblock plus) of tracking blockers (zoals Ghostery of Privacy Badger) kunnen als extensie in de browser geïnstalleerd worden.

7.2 Gebruik geen privacygevoelige informatie in file en folder namen

Gebruik geen namen van personen of andere privacygevoelige informatie in bestandsnamen of folders. Dit advies staat ook beschreven in https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf

8 Data Transfer Impact Assesment

Eén van de punten voortvloeiend uit de DPIA in 2021, is de verzending van gegevens naar de Verenigde Staten. Voor dit punt is een apart traject gestart, de zogenaamde Data Transfer Impact Assessment (DTIA). Hierbij worden privacyrisico's onderzocht van doorgifte van gegevens naar landen buiten de Europese Economische Ruimte (EER).

Het onderzoek is uitgevoerd op Google Meet.

Voor de DTIA is gebruikt gemaakt van her Rosenthal model. Met dit model worden 6 soorten verwerkingen beoordeeld: https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx

1. de inhoudelijke gegevens (Content Data)
2. de Accoungegevens (zoals e-mail adres, naam en wachtwoord)
3. Helpdesk gegevens (Support Data),
4. Diagnostische Gegevens (over het individuele gebruik van Workspace)
5. Securitygegevens die Google in Amerika verwerkt, ook over klachten, en
6. Website gegevens (zoals cookies).

De DTIA concludeert dat er geen grote risico's zijn voor de overdracht van persoonsgegevens via Meet.

Er zijn nog een aantal belangrijke maatregelen die de scholen zelf moeten nemen om de doorgifte-risico's te verkleinen.

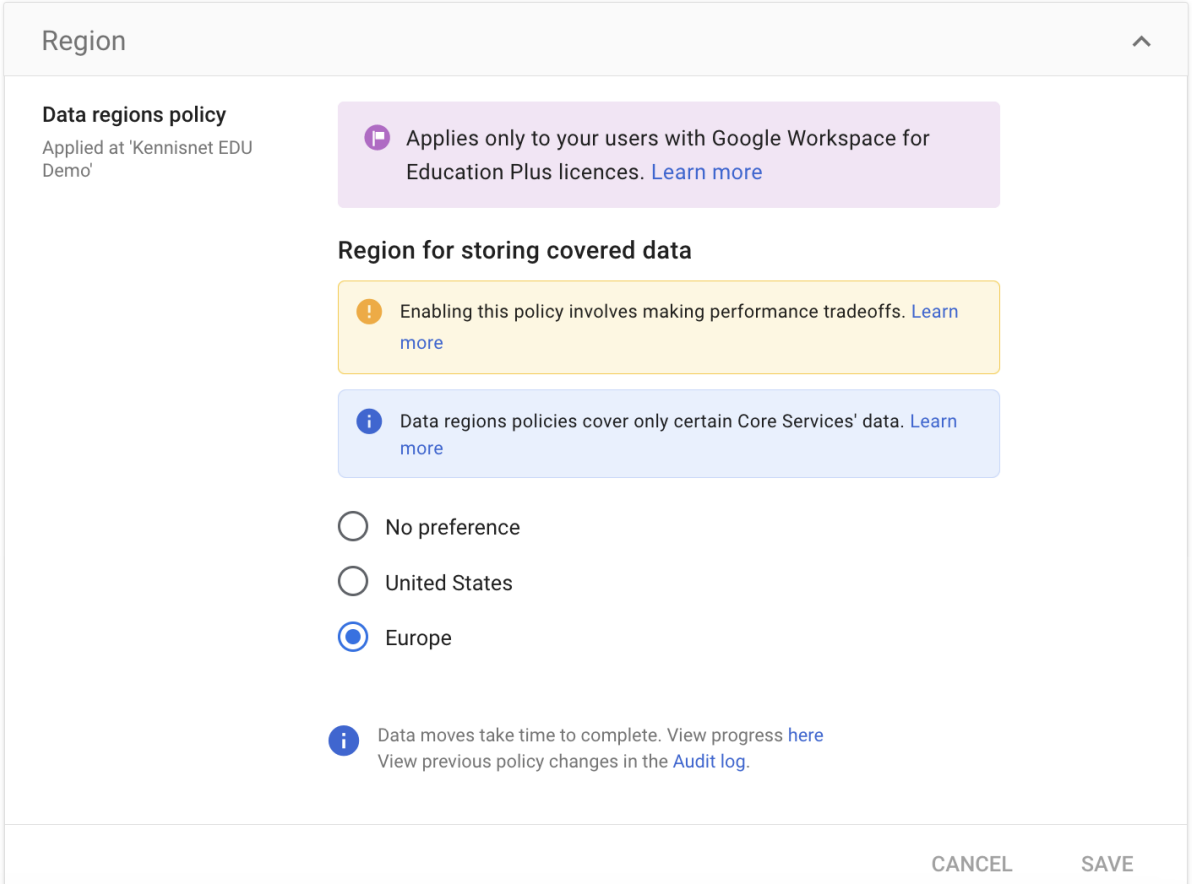
- kiezen voor opslag van de Inhoudelijke Gegevens in de EU.
- Als de organisaties verwachten dat de gebruikers bijzondere persoonsgegevens willen uitwisselen via Meet, moeten ze Client Side Encryption toepassen, met lokaal sleutelbeheer,

om het risico van ongeautoriseerde toegang tot deze gegevens in 7 derde landen volledig uit te sluiten.

8.1 Data regions

Login als beheerder op admin.google.com en ga naar Account > Account settings > Data regions -> selecteer Europa

Deze functionaliteit is niet beschikbaar in Google Workspace for Education fundamentals, een upgrade naar Google Workspace for education standard of plus is noodzakelijk om data regions te kunnen selecteren.



8.2 Client Side Encryption

Scholen die bijzondere persoonsgegevens willen verwerken in Google Workspace moeten Client Side Encryption toepassen, met lokaal sleutelbeheer, om het risico van ongeautoriseerde toegang tot deze gegevens in 7 derde landen volledig uit te sluiten.

Dit risico bestaat bij de risico beoordeling van content data: *Risk assesment on Content Data: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider*

Het probleem met encryptie in de cloud is dat de sleutel in bezit is van Google. Hierdoor kan Google op grond van verschillende wetten toegang geven tot klantdata aan overheidsinstanties.

Google houdt twee rapporten bij over het verstrekken van gegevens.

1) Wereldwijd, Amerika uitgezonderd: https://transparencyreport.google.com/user-data/overview

2) Amerika: https://transparencyreport.google.com/user-data/us-national-security

Hoe Google omgaat met verzoeken om gebruikersgegevens met betrekking tot de nationale veiligheid in de Verenigde Staten: https://policies.google.com/terms/information-requests

Met client side encryption wordt data nogmaals versleuteld met een sleutel die niet in de Google cloud staat. Google is dan niet meer in staat data van klanten in een leesbaar formaat aan overheidsinstanties te leveren.

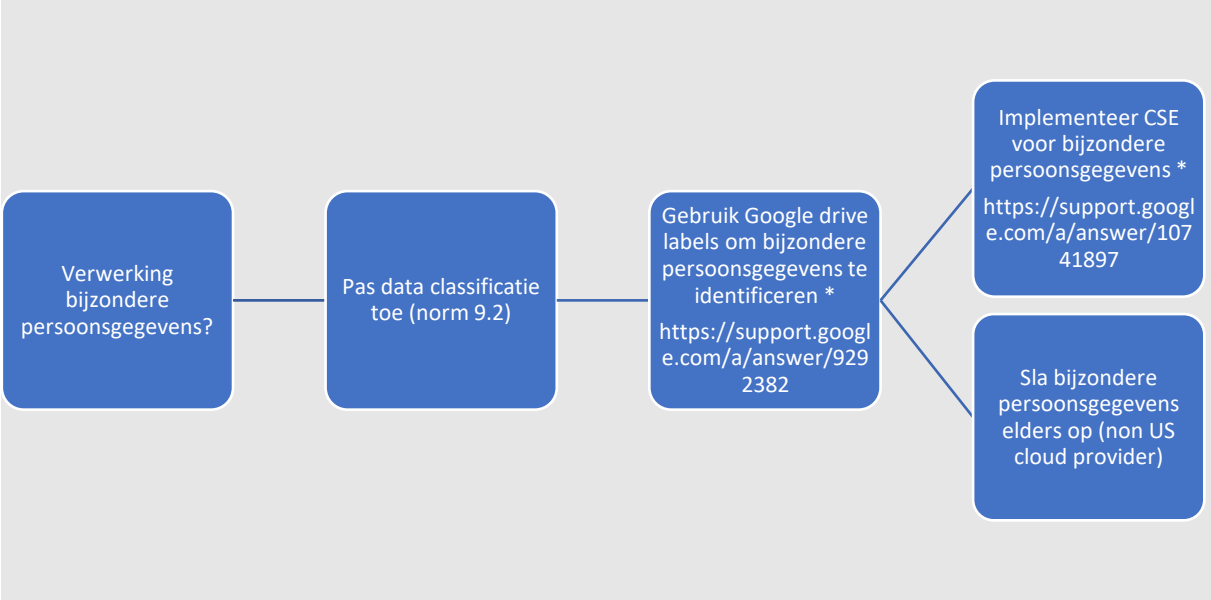
CSE Encryptie versleuteld alleen de content data. Metadata, zoals file names, labels en de accesscontrol list blijft leesbaar voor Google.

Met CSE wordt de data encryption key (DEK) versleuteld met een key encryption key (KEK).

De KEK wordt beheerd door een key management systeem extern aan de Google omgeving.

Bron: https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf

Aanpak:



We adviseren scholen ten eerste data te classificeren. Data classificatie staat beschreven in de normen van van het IBP normenkader van Domein 9 “Data Management”. Data classificatie is nodig om informatie te classificeren (gewone gegevens, bijzondere gegevens, etc.) zodat het juiste beschermingsniveau kan worden toegepast. Met de gratis licentie van Google Workspace (fundamentals) kan data in Google drive niet geclassificeerd worden. Hiervoor is minimaal de Google Workspace for Education Standard nodig.

https://support.google.com/a/answer/9292382?hl=en&fl=1&sjid=98660791415985355-NA De feature heet: Drive labels and classification.

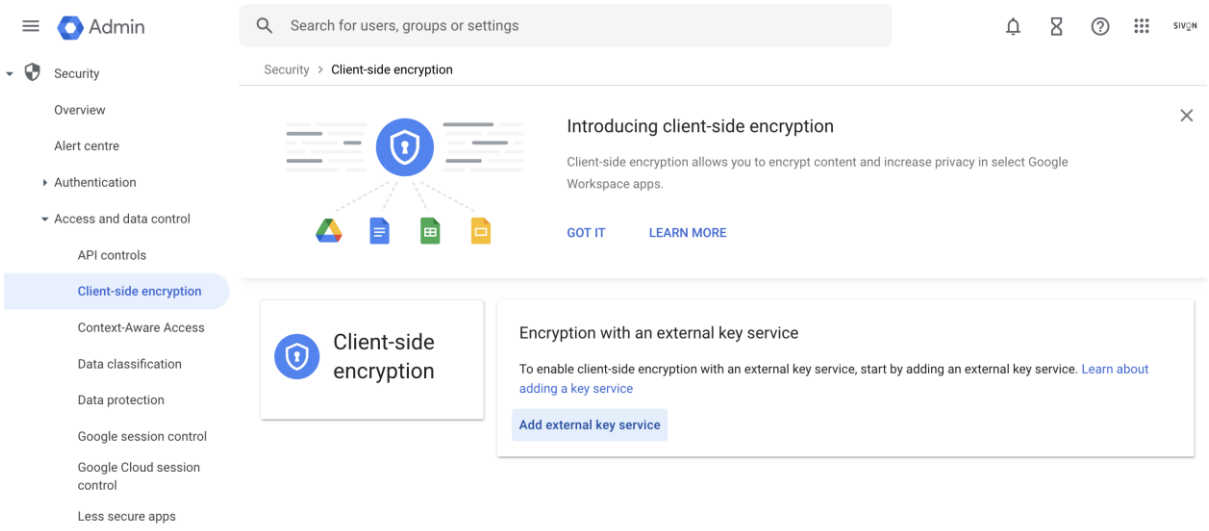
Indien scholen bijzondere persoonsgegevens verwerken in Google Workspace zal voor deze gegevens client side encryption (CSE) geimplementeerd moeten worden. CSE geeft een extra laag encryptie waarbij sleutel in beheer is buiten de Google omgeving.

Naast CSE in Google Workspace zal er een dienst (key service) gekoppeld moeten worden om extern sleutel beheer mogelijk te maken. Met CSE kan de sleutel namelijk niet in de Google cloud opgeslagen worden.

Er zijn drie Europese leveranciers die key services aanbeiden:

- Stormshield
- Flowcrypt
- Thales

Om CSE te activeren log in als beheerder en ga naar: Security > Access and data control > Client-side encryption



Sommige functies zijn niet beschikbaar zijn bij gebruik van CSE.

Beperkingen bij Drive/Doc/Sheets

- Spelling en gramatica check in Google Docs Editors
- Editing met meerdere gebruiks op hetzelfde moment
- Search
- Commentaar toevoegen

Beperkingen bij Gmail

- Confidential mode
- Sending to groups as recipients
- Doorzoeken van berichten
- E-mail signatures
- Print

- email delegation (shared inboxes)

Beperkingen bij Kalender

- Doorzoeken van kalender
- Encrypting of decrypting events offline

Beperkingen bij Meet

- Meetings opnemen
- Live streams
- Inbellen voor audio
- Polls
- Jamboard
- "Knocking" https://workspaceupdates.googleblog.com/2020/08/block-google-meet-participants-from.html
- Gebruik van meeting room hardware
- Uitnodigingen voor deelnemers buiten de organisatie

Colofon

Technische handleiding voor Google Workspace for Education

Datum van uitgave
2 augustus 2021 (versie 1.0)
20 juli 2023 (versie 2.0)
31 augustus 2023 (versie 2.1)
27 februari 2024 (versie 3.0)

Auteurs
Versie 1.0: Hans-Peter Ligthart (Kennisnet), Job Vos (SIVON), Theresa Song Loong (Kennisnet)
Versie 2.0: Hans-Peter Ligthart (SIVON)

SIVON en Kennisnet worden gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

Deze publicatie is tot stand gekomen in samenwerking met SURF. **SIVON** helpt scholen bij het realiseren en doorontwikkelen van veilig en toekomstbestendig digitaal onderwijs, nu en in de toekomst; zij adviseert, ontzorgt en behartigt de belangen van scholen, zodat die zich kunnen richten op hun primaire taak: het verzorgen van het allerbeste onderwijs.

sivon.nl