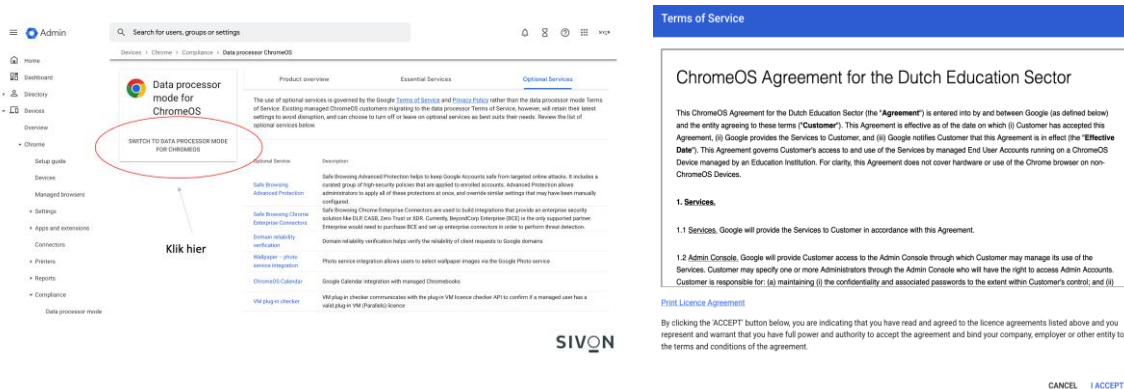


## Chrome privacyhandleiding

In mei 2023 hebben SIVON en Google overeenstemming bereikt over een nieuwe verwerkersversie voor Chrome OS en Chrome-browser op Chrome-apparaten.

Om een aantal belangrijke privacyrisico's bij het gebruik van Chrome af te dekken, dienen scholen onderstaande maatregelen te nemen:

- 1) accepteer de nieuwe verwerkersovereenkomst 'ChromeOS Agreement for the Dutch Education Sector'. Nederlandse educatie-instelling worden hierover geïnformeerd door Google. De overeenkomst is ook te vinden in de admin console (zie afbeelding);



- 2) breng alle Chrome-apparaten onder beheer bij een Workspace tenant met de 'Chrome Education Upgrade' licentie. Deze licentie maakt centraal beheer van Chromebooks mogelijk. Alleen centraal beheerde Chromebooks kunnen als verwerkersversie geconfigureerd worden;
- 3) implementeer onderstaande instellingen voor jouw Google-omgeving.

## Chrome Education Upgrade

Scholen kunnen alleen verwerkersverantwoordelijken zijn en Google verwerker als de door de scholen gebruikte apparaten in beheer zijn genomen. Je kunt je Chrome-apparaten in beheer nemen met de zogenaamde Chrome Education Upgrade. Dit is feitelijk een Enterprise editie van Chrome OS.

Chromebooks kennen een zogenaamde Update Expiration Date (AUE)

<<https://support.google.com/chrome/a/answer/6220366>>. Deze datum kun je zien als het einde van de levensduur van het apparaat. Als er geen updates meer beschikbaar zijn voor het apparaat, dien je het dus te vervangen. Schoolbesturen dienen een overweging te maken of een apparaat dat nog niet in beheer is maar wel dicht tegen de houdbaarheidsdatum zit, alsnog in beheer nemen of direct vervangen. Apparaten waarvan de AUE-datum al is gepasseerd, dienen sowieso te worden vervangen.

De standaardinstelling is dat Chrome OS automatisch software-updates uitvoert. Handhaaf deze instelling.

N.B.: het in beheer nemen van apparaten is ook één van de te nemen maatregelen voor mobiele apparaten zoals in norm 11.3 van het normenkader: *'mobile device management of mobile application management (MDM/MAM) wordt gebruikt voor het beveiligen van mobiele apparaten of telewerkfaciliteiten. Dit wordt opgenomen in het IBP-beleid (norm 1.2). Het MDM of MAM moet dusdanig zijn ingesteld dat invulling wordt gegeven aan de elementen van het toetsingskader.'*

## Acties voor admins

Dit zijn maatregelen die scholen centraal moeten instellen.

Voor de verwerker versie (data processor) van Chrome heeft Google een nieuwe compliance pagina ingericht. Deze pagina is te vinden onder Chrome -> Compliance -> Data processor

<https://admin.google.com/u/1/ac/chrome/compliance/productoverview>

**Data processor ChromeOS**  
You are in control of your own personal data.

**Product overview**

Switching to the data processor mode Terms of Service makes Google primarily a data processor under the General Data Protection Regulation (GDPR) for personal data handled by essential services, giving customers greater control over when, how and why their data is processed by Google. The essential services are the base features and applications required to provide a reliable and secure experience across ChromeOS.

As a data processor, Google may only process personal data contained in customer data or the service data of essential services to provide, maintain, improve and update Chrome, to fix bugs or other security threats, or as otherwise allowed by customers (such as when a setting is changed). Service data may also be processed by Google as a data controller for specific, limited legitimate business purposes detailed in the data processor mode Terms of Service, such as billing and account management, technical support or abuse detection.

For managed ChromeOS customers, we offer a way to turn off all optional services at once, since Google remains a data controller for the personal data processed by such services. The use of optional services is governed by the Google Terms of Service and Privacy Policy rather than the data processor mode Terms of Service. Existing managed ChromeOS customers migrating to the data processor mode Terms of Service, however, will retain their latest settings to avoid disruption and can choose to turn off or leave on optional services as best suits their needs.

To make the switch, review and accept the data processor mode Terms of Service and review the optional services.

Features/capabilities	Description
<a href="#">Download service data</a>	Allows administrators to download a copy of a user's service data.
<a href="#">Takeout customer data</a>	Allows administrators to search and download a copy of a user's customer data.
<a href="#">Delete user data</a>	Allows administrators to delete a user's in-scope data when deleting a user account.

Op deze pagina staan de essential services die onder de nieuwe overeenkomst met Google vallen en waar Google verwerker is.

De optional services vallen niet onder de nieuwe overeenkomst. Google is voor deze diensten nog verantwoordelijke. Google heeft zogenaamde switches ontwikkeld zodat admin's de optional services uit kunnen zetten.

### Zet optional services' uit

Voor nieuwe Google tenants is de default waarde 'uit'. Voor bestaande tenants moeten admins de optional services uit zetten. Het gaat hierbij alleen om optional services waarbij persoonlijke data worden verwerkt.

Vanuit het menu optional services zoals hierboven weergegeven kan je doorklikken naar de diverse settings en daar de service uit zetten. Hieronder staan een 3tal voorbeelden. Elke dienst kan individueel uitgezet worden.

**Nearby Share** ⓘ  
Locally applied ▼  
Prevent users from enabling Nearby Share ▼

**Google Calendar integration** ⓘ  
Locally applied ▼  
Disable Google Calendar integration ▼

## Spell check service

Locally applied ▼



Disable the spell checking web service ▼

Er is ook een “uber-switch”. Deze is alleen beschikbaar voor nieuwe tentants. Met deze switch kunnen alle optional services in een keer uit gezet kunnen worden. **Let op!** Als optional service nu gebruikt worden kan het gebruik van de uber switch tot verlies van functionaliteit of data leiden.

### Gebruik altijd K-12 settings

Met een K-12 setting zorg je als school voor de best mogelijke privacy-instellingen. Hanteer voor alle leerlingen en bij voorkeur ook voor alle medewerkers deze setting. Een uitzondering zijn de administrator accounts.

Met de K-12 setting bescherm je je organisatie tegen experimenten met een nieuwe technologie die Privacy Sandbox heet. Privacy Sandbox is een manier om persoonlijke advertenties te kunnen tonen zonder 3rd party cookies te gebruiken. Google zegt géén trials te doen met Privacy Sandbox onder gebruikers die vallen onder de K-12 instellingen. Voor gebruikers die in Workspace gemarkeerd zijn als ouder dan 18 jaar, kun je Privacy Sandbox lokaal uitzetten.

In de admin console -> Account settings -> Age based settings

Age-based access settings ^

---

**Age label**  
Applied at 'Kennisnet EDU Demo'

Choose an appropriate age label  
Your **organization type** determines the default setting selected here for groups and org units. Specify a different age label if the default setting does not apply for a group or org unit. [Learn more about age-based access settings](#)

**Some or all users in this group or org unit are under 18**  
Access to some Google services or features may be restricted and data in those services or features may be deleted for users in the group or org unit

**All users in this group or org unit are 18 or older**  
Don't select if this group or org unit has any users under 18

**i** Most changes take effect within a few minutes. [Learn more](#)  
You can view prior changes in the [audit log](#)

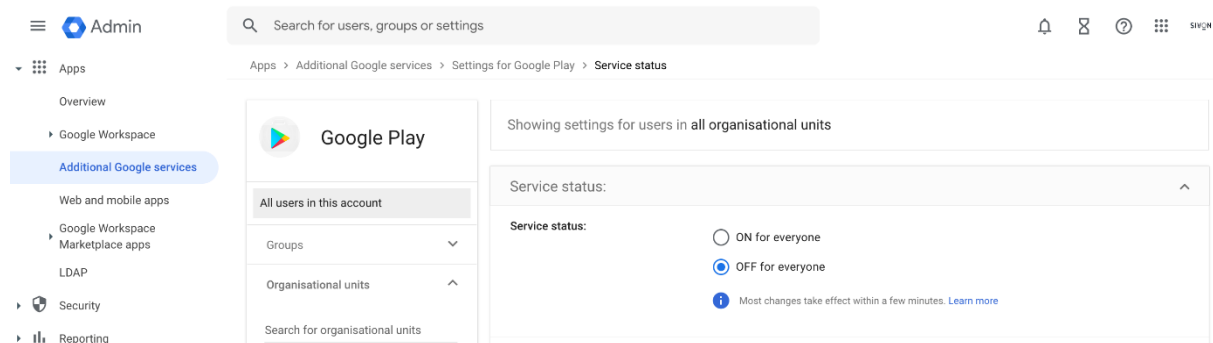
CANCEL    SAVE

### Zet de Chrome Web Store uit

De Chrome web store valt niet onder de verwerkersovereenkomst. Default staat de Chrome web store uit.

### Zet de Google Play uit

De Google play valt niet onder de verwerkersovereenkomst. Google Managed play is een processor service. Tijdens het Chrome onderzoek hebben we niet kunnen vaststellen of de dienst zonder hoge risico's te gebruiken is.



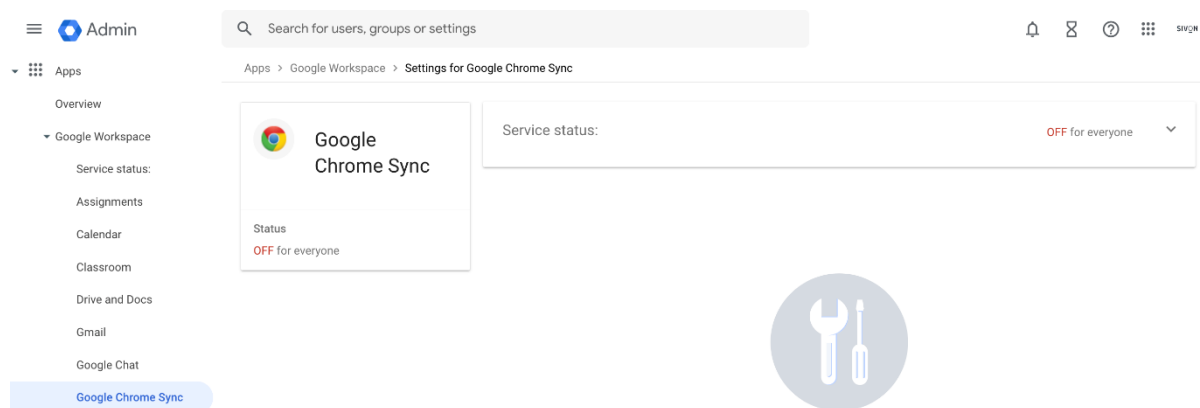
### Zet ad personalisatie uit. Voor K-12 is dit de default waarde

K-12 instellingen moet voor alle po- en vo-scholengelden. Voor niet K-12 scholen volg de instructie zoals hier beschreven <https://support.google.com/a/answer/6304811?hl=en>

### Zet Chrome Sync uit

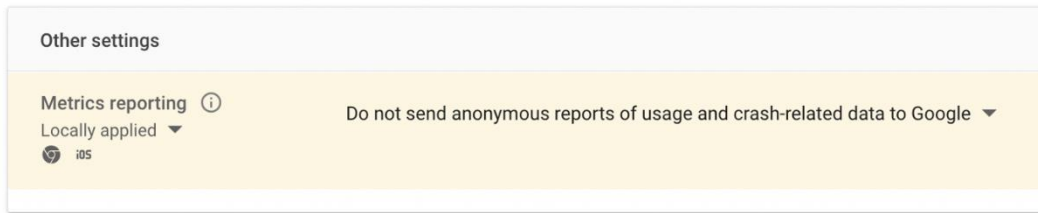
Met Chrome Sync kan gevoelige data verwerkt worden. Er zijn 3 opties om de privacy risico's te mitigeren:

- 1) Zet Chrome sync uit
- 2) Gebruikt Chrome sync encryptie (gebruiker moet dit zelf instellen)
- 3) Wacht op de release van client side encryptie van Chrome Sync



### Verstuur geen "crash report" naar Google

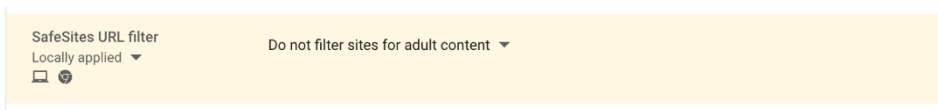
Onder devices -> chrome -> settings -> users and browser gebruik de instelling "stuur geen crash reports" naar Google.



### Overweeg “safe sites” uit te zetten en een andere filter functie te implementeren

Safe Sites is een essential service en valt daarmee onder de verwerkersovereenkomst. Volgens Google wordt er geen data opgeslagen als url gecontroleerd worden door Safe sites. “Google stated it did not collect any personal identifiers with the URLs and did not store the URLs “. We hebben dit niet kunnen verifiëren. Hier zit een mogelijk risico.

Onder devices -> chrome -> settings -> users and browser kan je de SafeSites URL filter uit zetten. Implementeer dan een andere filterfunctie om toegang tot adult content te blokkeren.



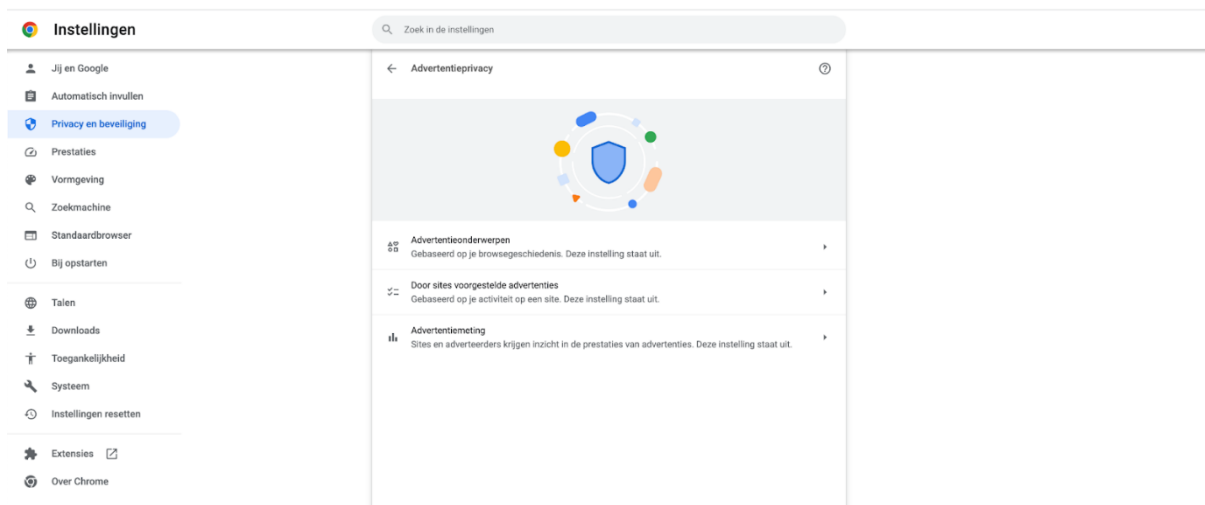
## User acties

Dit zijn instellingen die de eindgebruikers zelf moet doorvoeren

### Switch off privacy sandbox.

Privacy Sandbox is een nieuwe ontwikkeling voor het presenteren van persoonlijke advertenties zonder het plaatsen van 3rd party cookies. Google zal geen trials doen met de Privacy Sandbox voor gebruikers die van onder de K-12 instellingen vallen. Voor gebruikers die in Workspace gemarkeerd zijn als ouder dan 18 kan de Privacy Sandbox lokaal uitgezet worden zoals hieronder beschreven.

Ga in de browser naar instellingen -> Privacy en beveiliging -> Advertentieprivacy (voorheen Privacy sandbox).



Elke functie kan afzonderlijk aan en uit gezet worden.

### Zet advertentieonderwerpen uit

**Instellingen** Zoek in de instellingen

- Jij en Google
- Automatisch invullen
- Privacy en beveiliging**
- Prestaties
- Vormgeving
- Zoekmachine
- Standaardbrowser
- Bij opstarten

---

- Talen
- Downloads
- Toegankelijkheid
- Systeem
- Instellingen resetten
- Extensies
- Over Chrome

**← Advertentieonderwerpen**

**Advertentieonderwerpen**  
Interessante onderwerpen zijn gebaseerd op je recente browsegeschiedenis en worden door sites gebruikt om gepersonaliseerde advertenties te tonen

**Je onderwerpen**  
Je kunt onderwerpen blokkeren die je niet wilt delen met sites. Chrome verwijdert ook automatisch onderwerpen die ouder zijn dan 4 weken. [Meer informatie](#)

Als deze optie aanstaat, zie je hier een lijst met onderwerpen op basis van je recente browsegeschiedenis

**Onderwerpen die je hebt geblokkeerd**

Of een advertentie wordt gepersonaliseerd terwijl je browsat, is afhankelijk van deze instelling, [door sites voorgestelde advertenties](#), je [cookie-instellingen](#) en of de site die je bekijkt advertenties personaliseert

## Zet door sites voorgestelde advertenties uit

**Instellingen** Zoek in de instellingen

- Jij en Google
- Automatisch invullen
- Privacy en beveiliging**
- Prestaties
- Vormgeving
- Zoekmachine
- Standaardbrowser
- Bij opstarten

---

- Talen
- Downloads
- Toegankelijkheid
- Systeem
- Instellingen resetten
- Extensies
- Over Chrome

**← Door sites voorgestelde advertenties**

**Door sites voorgestelde advertenties**  
Sites die je bezoekt, kunnen vaststellen wat je leuk vindt en daarna advertenties voorstellen terwijl je verder browsat

**Sites**  
Je kunt ongewenste sites blokkeren. Chrome verwijdert sites die ouder zijn dan 4 weken ook automatisch uit de lijst. [Meer informatie](#)

Als deze optie aanstaat, zie je hier een lijst met sites die je bezoekt en die je interesses raden

**Sites die je hebt geblokkeerd**

Of een advertentie wordt gepersonaliseerd terwijl je browsat, is afhankelijk van deze instelling, [advertentieonderwerpen](#), je [cookie-instellingen](#) en of de site die je bekijkt advertenties personaliseert

## Zet advertentiemeting uit

**Instellingen** Zoek in de instellingen

- Jij en Google
- Automatisch invullen
- Privacy en beveiliging**
- Prestaties
- Vormgeving
- Zoekmachine
- Standaardbrowser
- Bij opstarten

---

- Talen
- Downloads
- Toegankelijkheid
- Systeem
- Instellingen resetten
- Extensies
- Over Chrome

**← Advertentiemeting**

**Advertentiemeting**  
Sites en adverteerders kunnen de prestaties van hun advertenties meten

**Als dit aanstaat**

- Es worden beperkte typen gegevens gedeeld tussen sites om de prestaties van hun advertenties te meten (bijvoorbeeld het tijdstip waarop je een advertentie werd getoond)
- De gegevens van advertentiemetingen worden regelmatig van je apparaat verwijderd
- Je browsegeschiedenis blijft privé op je apparaat en rapporten worden met vertraging verstuurd om je identiteit te beschermen

**Overwegingen**

- Je kunt de gegevens van advertentiemetingen altijd verwijderen door je browsegegevens te verwijderen
- Chrome beperkt de totale hoeveelheid gegevens die sites via de browser kunnen delen om de advertentieprestaties te meten
- Je Android-apparaat kan een vergelijkbare instelling hebben. Als advertentiemeting aanstaat in Chrome en op je Android-apparaat, kan een bedrijf mogelijk de effectiviteit van een advertentie meten op websites die je bezoekt en in apps die je gebruikt.

## Privacy Sandbox



**Proeven**

Met een Privacy Sandbox-proef kunnen sites dezelfde browsefunctionaliteit leveren terwijl er minder van je gegevens worden gebruikt. Dit betekent meer privacy voor jou en minder tracking op meerdere sites. Als andere proeven klaar zijn om te worden getest, voegen we deze toe. [Over browsergebaseerde advertentiepersonalisatie](#)

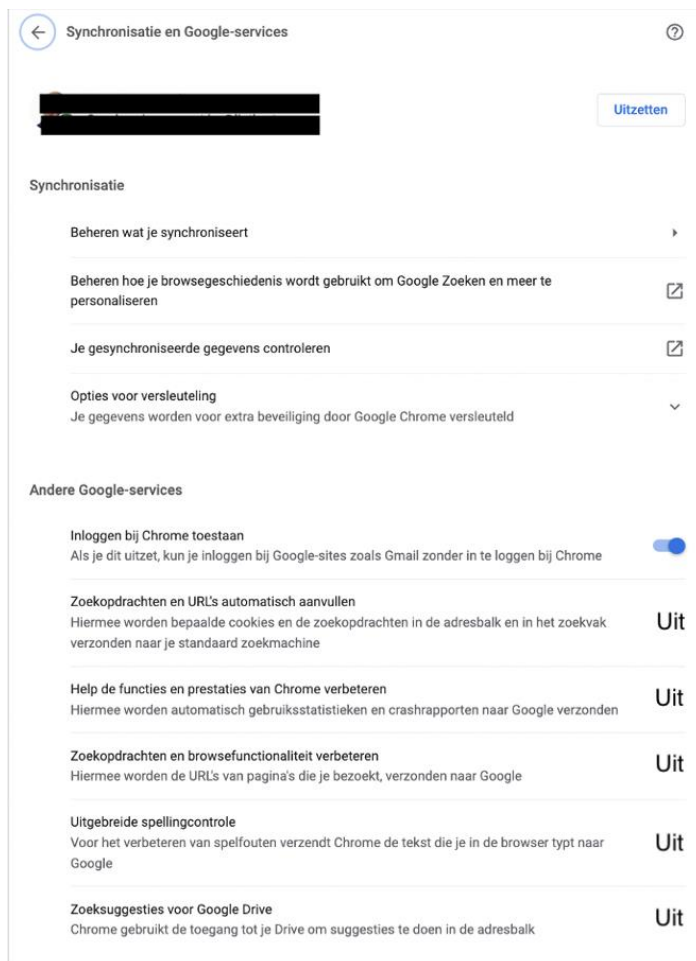
- Browsergebaseerde advertentiepersonalisatie**  
Je browsegeschiedenis heeft invloed op de advertenties die je ziet
- Advertentiemeting**  
Adverteerders kunnen inzicht krijgen in hoe advertenties presteren
- Spam- en fraudebeperking**  
Help sites fraude te bestrijden en bots te onderscheiden van mensen

Bij gebruik van Chrome sync moet de data encrypt worden.

The screenshot shows the Chrome settings page for 'Synchronisatie en Google-services'. The left sidebar lists various settings categories like 'Jij en Google', 'Automatisch invullen', 'Privacy en beveiliging', etc. The main content area is titled 'Synchronisatie en Google-services' and includes a search bar. Below the search bar, there is a section for 'Synchronisatie' with several options: 'Beheren wat je synchroniseert', 'Beheren hoe je browsegeschiedenis wordt gebruikt om Google Zoeken en meer te personaliseren', 'Je gesynchroniseerde gegevens controleren', and 'Opties voor versleuteling'. The 'Opties voor versleuteling' section is expanded, showing two radio button options: 'Gesynchroniseerde wachtwoorden versleutelen met je Google-account' (selected) and 'Gesynchroniseerde gegevens versleutelen met je eigen wachtwoordzin voor synchronisatie'.


## Gebruik privacy vriendelijke browsers settings

Verder adviseren we de volgende privacy vriendelijke browser settings te gebruiken



### 'Niet bijhouden' uitschakelen (do not track) en website preloading disables

Wanneer u je op internet browserd op computers of Android-apparaten, kun je een verzoek naar websites verzenden om jouw browsegegevens niet te verzamelen of bij te houden. De functie is standaard uitgeschakeld.

- 4) Open Chrome op je computer.
- 5) Klik rechtsboven op Meer  > **Instellingen**.
- 6) Klik op **Privacy en beveiliging** > **Cookies en andere sitegegevens**.
- 7) Zet **Een verzoek voor niet bijhouden met je browseverkeer verzenden** aan of uit.



## Instellingen


Zoek in de instellingen

- Jij en Google
- Automatisch invullen
- Privacy en beveiliging**
- Prestaties
- Vormgeving
- Zoekmachine
- Standaardbrowser
- Bij opstarten
- Talen
- Downloads
- Toegankelijkheid
- Systeem
- Instellingen resetten

Alle cookies toestaan

Cookies van derden blokkeren in incognitomodus

Cookies van derden blokkeren

 Sites mogen cookies gebruiken om de browsefunctionaliteit te verbeteren, bijvoorbeeld door je ingelogd te houden of door artikelen in je winkelwagen te onthouden

Sites kunnen je cookies niet gebruiken om je browse-activiteit op verschillende sites te bekijken, bijvoorbeeld om advertenties te personaliseren. Functies op bepaalde sites werken misschien niet.

Alle cookies blokkeren (niet aanbevolen)

Cookies en sitegegevens wissen als je alle vensters sluit  
Als de schakelaar aanstaat, word je ook uitgelogd van Chrome

Een verzoek voor 'Do Not Track' met je browseverkeer verzenden

Pagina's vooraf laden voor sneller browsen en zoeken  
Hiermee worden de pagina's die je volgens Chrome misschien wilt bezoeken, vooraf geladen. Chrome kan hiervoor gebruikmaken van cookies, als je cookies toestaat, en de pagina's versleutelen en versturen via Google, zodat je identiteit verborgen blijft voor sites. 