

Google-Handbuch

ChromeOS und Chrome

Browser

Version 2.0 Februar 2024

Inhaltsverzeichnis

1 Einleitung	3
2 ChromeOS-Verarbeitungsvereinbarung	3
3 Chrome Education-Upgrade	3
4 Datenschutzeinstellungen für ChromeOS und Chrome-Browser	4
<i>„Optionale Dienste“ deaktivieren</i>	<i>5</i>
<i>Verwenden Sie immer die K-12-Einstellungen</i>	<i>5</i>
<i>Deaktivieren Sie den Chrome Web Store</i>	<i>6</i>
<i>Google Play ausschalten</i>	<i>6</i>
<i>Deaktivieren Sie die personalisierte Werbung. Für K-12 ist dies der Standardwert</i>	<i>7</i>
<i>Senden Sie keinen „Absturzbericht“ an Google</i>	<i>7</i>
<i>Erwägen Sie die Deaktivierung von „Sicheren Websites“ und die Implementierung einer anderen Filterfunktion.</i>	<i>7</i>
5 Endbenutzereinstellungen	8
<i>Privacy Sandbox ausschalten</i>	<i>8</i>
<i>Anzeigenthemen deaktivieren</i>	<i>8</i>
<i>Von Websites vorgeschlagene Anzeigen deaktivieren</i>	<i>9</i>
<i>Anzeigenmessung deaktivieren</i>	<i>9</i>
<i>Chrome-Sync-Verschlüsselung verwenden</i>	<i>10</i>
6 Datenschutzfreundliche Browsereinstellungen verwenden	11
<i>Durch die Deaktivierung von „Do Not Track“ und dem Vorladen der Website wird die Funktion deaktiviert</i>	<i>11</i>

Versionsverwaltung

3. Juli 2023 (Version 1.0)	Erste Version des Handbuchs
27. Februar 2024 (Version 2.0)	Änderung im Layout Update nach Überprüfung der von Google gelieferten Produktänderungen. Google hat die Produkt-Änderungen adäquat umgesetzt. Die Überprüfung hat keine Auswirkungen auf die Maßnahmen, die von den Schulen durchgeführt werden müssen. Die Schulen sollten weiterhin die Maßnahmen in diesem Leitfaden befolgen.

1 Einleitung

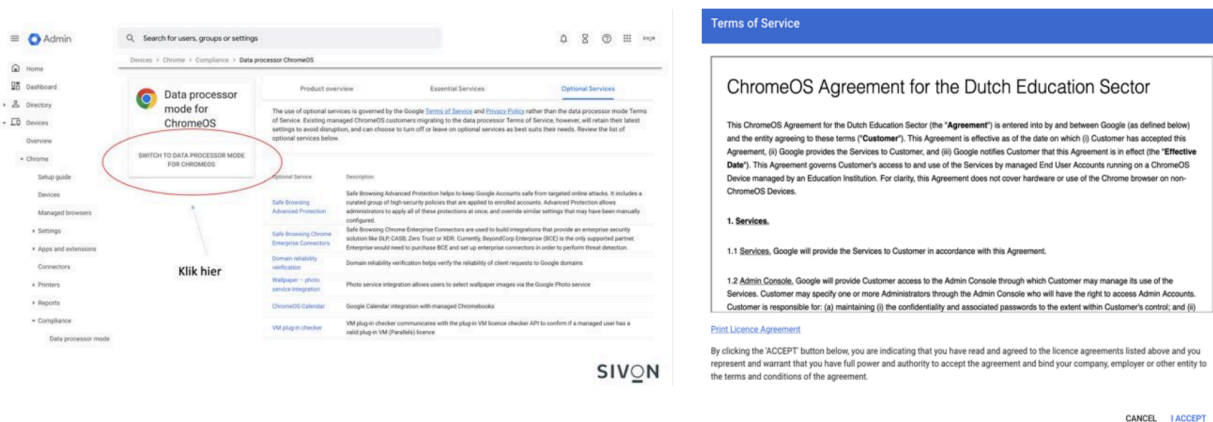
Im Mai 2023 einigten sich SURF und SIVON mit Google auf die neuen Nutzungsbedingungen (Terms of Service; ToS) für die Nutzung von ChromeOS und Chrome-Browser für Chromebooks. Sobald Sie als Schulleitung diese Vereinbarung akzeptiert und die Kontrolle über die Chromebooks übernommen haben, ist Google ein Auftragsverarbeiter und Sie als Schulleitung ein Verantwortlicher für die Verarbeitung personenbezogener Daten auf Chromebooks (die unter ChromeOS laufen) und in Chrome-Browsern (die auf Chromebooks laufen). Durch die Annahme dieser Vereinbarung und die Umsetzung der damit verbundenen Maßnahmen verringern Sie die Datenschutzrisiken für Schüler und Mitarbeiter bei der Verwendung von Chromebooks mit ChromeOS und dem Chrome-Browser.

Die sogenannte Datenverarbeiter-Version von Chrome¹ (Data Processor; DP Chrome OS) ist seit dem 12. August 2023 verfügbar.

Die neuen Datenschutzbestimmungen gelten nur für die sogenannten wichtigen Dienste (Essential Services)².

2 ChromeOS-Verarbeitungsvereinbarung

Akzeptieren Sie die neue Verarbeitungsvereinbarung „ChromeOS-Vereinbarung für den niederländischen Bildungssektor“³. Niederländische Bildungseinrichtungen wurden von Google darüber informiert. Die Vereinbarung finden Sie in der Admin-Konsole (siehe Bild);



3 Chrome Education-Upgrade

Schulen können nur dann als Verantwortliche und Google als Auftragsverarbeiter fungieren, wenn die von den Schulen verwendeten Geräte verwaltet werden. Sie können Ihre Chrome-Geräte mit dem sogenannten Chrome Education Upgrade in die Verwaltung aufnehmen. Dabei handelt es sich eigentlich um eine Enterprise-Edition von Chrome OS.

Chromebooks haben ein sogenanntes Update Expiration Date (AUE)

<https://support.google.com/chrome/a/answer/6220366?hl=en>. Sie können dieses Datum als das Ende der Lebensdauer des Geräts betrachten. Wenn also keine Updates mehr für das Gerät

¹ Siehe <https://support.google.com/chrome/a/answer/14316192?hl=de&sjid=15109340273151152981-EU>

² Siehe <https://support.google.com/chrome/a/answer/13598068?hl=de&sjid=15109340273151152981-EU>

³ Mit Stand von 16.10.2024 auch in Deutschland verfügbar, einfach als "Datenverarbeitermodus" unter Geräte> Chrome> Compliance

verfügbar sind, müssen Sie es ersetzen. Schulleitungen müssen abwägen, ob ein Gerät, das noch nicht verwaltet wird, aber kurz vor dem Verfallsdatum steht

noch verwaltet oder sofort ersetzt werden sollte. Geräte, deren AUE-Datum bereits überschritten ist, sollten auf jeden Fall ersetzt werden.

Die Standardeinstellung ist, dass Chrome OS Software-Updates automatisch durchführt. Behalten Sie diese Einstellung bei.

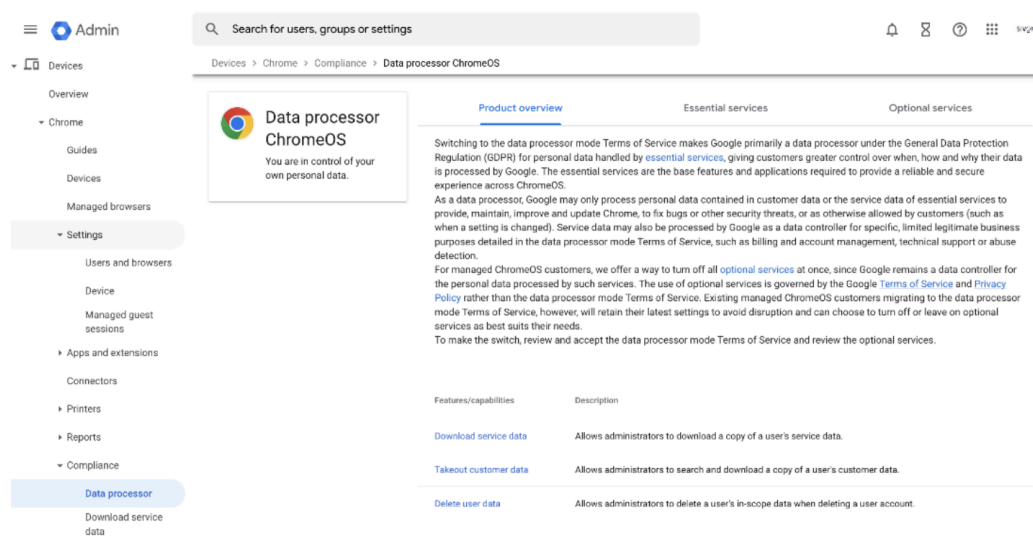
Hinweis: Die Pflege von Geräten ist auch eine der Maßnahmen, die für mobile Geräte gemäß Standard 11.3 des Standardrahmens ergriffen werden müssen: *Mobile Device Management oder Mobile Application Management (MDM/MAM) dient der Absicherung mobiler Geräte oder Telearbeitseinrichtungen. Dies ist in der IBP-Richtlinie (Standard 1.2) enthalten. „Das MDM bzw. MAM muss so eingerichtet sein, dass die Elemente des Bewertungsrahmens erfüllt werden.“*

4 Datenschutzeinstellungen für ChromeOS und Chrome-Browser

Dies sind Maßnahmen, die Schulen zentral umsetzen müssen.

Google hat eine neue Compliance-Seite für die Datenverarbeiterversion (data processor) von Chrome eingerichtet. Diese Seite finden Sie unter **Chrome -> Compliance -> Datenverarbeiter**

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



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

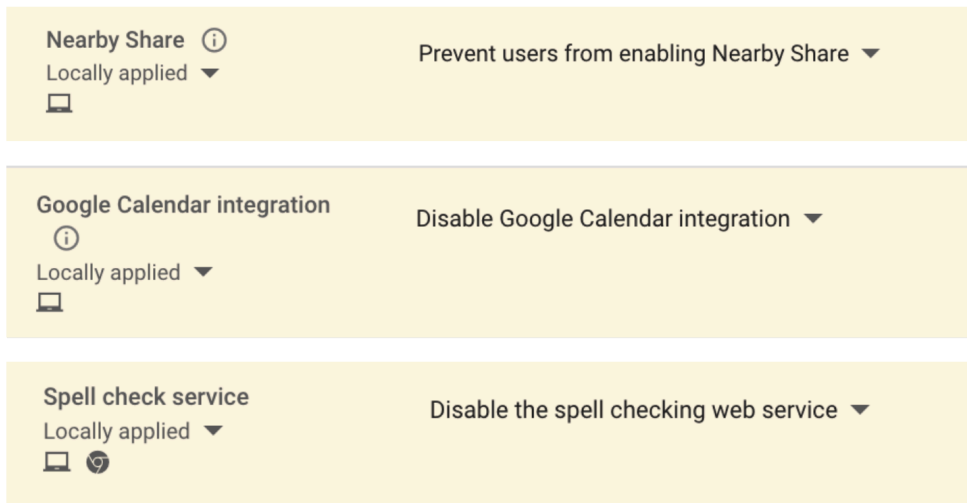
Auf dieser Seite werden die wichtigen Dienste (essential services) aufgeführt, die unter die neue Vereinbarung mit Google fallen und bei denen Google als Auftragsverarbeiter fungiert.

Die optionalen Dienste (optional services) fallen nicht unter die neue Vereinbarung. Für diese Dienste ist weiterhin Google verantwortlich. Damit Administratoren die optionalen Dienste deaktivieren können, hat Google sogenannte Schalter entwickelt.

„Optionale Dienste“ deaktivieren

Für neue Google-Tenants gilt: Standardwert 'aus'. Für bestehende Tenants müssen Administratoren die optionalen Dienste deaktivieren. Dies betrifft ausschließlich optionale Dienste, bei denen personenbezogene Daten verarbeitet werden.

Über das Menü für optionale Dienste (siehe oben) können Sie sich durch die verschiedenen Einstellungen klicken und den Dienst dort deaktivieren. Nachfolgend finden Sie drei Beispiele. Jeder Dienst kann einzeln deaktiviert werden.



Es gibt auch einen “Haupt-Schalter“. Dies gilt nur für neue Tenants. Mit diesem Schalter können alle optionalen Dienste auf einmal ausgeschaltet werden. **ACHTUNG!** Wird ein optionaler Dienst bereits genutzt, kann die Nutzung des Haupt-Schalters zu Funktions- oder Datenverlusten führen.

Verwenden Sie immer die K-12-Einstellungen

Mit einer K-12-Einstellung stellen Sie als Schule die bestmöglichen Datenschutzeinstellungen sicher. Nutzen Sie diese Einstellung für alle Schüler und vorzugsweise auch für alle Mitarbeiter. Eine Ausnahme bilden die Administratorkonten.

Mit der K-12-Einstellung schützen Sie Ihre Organisation vor Experimenten mit einer neuen Technologie namens Privacy Sandbox. Privacy Sandbox ist eine Möglichkeit, personalisierte Anzeigen zu schalten, ohne Cookies von Drittanbietern zu verwenden. Google sagt, dass es keine Versuche mit Privacy Sandbox bei Nutzern durchführen wird, die unter die K-12-Einstellungen fallen. Für Benutzer, die in Workspace als über 18 Jahre alt markiert sind, können Sie die Privacy Sandbox lokal deaktivieren.

In der **Admin-Konsole -> 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

Deaktivieren Sie den Chrome Web Store

Der Chrome Web Store fällt nicht unter die Verarbeitungsvereinbarung. Standardmäßig ist der Chrome Web Store deaktiviert.

The screenshot shows the Google Admin console interface. The search bar contains 'web store'. The breadcrumb trail is 'Apps > Zusätzliche Google-Dienste > Einstellungen für Chrome Web Store'. The main content area shows the 'Chrome Web Store' settings. A warning message states: 'Nutzungsbedingungen Dieser Dienst ist nicht Gegenstand der Google Workspace-Vereinbarung. Falls Sie nicht berechtigt sind, diesen Bedingungen im Namen des Kunden oder Endnutzers verbindlich zuzustimmen, deaktivieren Sie bitte den Dienst'. Below this, the 'Dienststatus' is set to 'Für alle DEAKTIVIERT'.

Schalten Sie Google Play aus

Google Play fällt nicht unter die Verarbeitungsvereinbarung. Google Managed Play ist ein Dienst, bei dem Google Verantwortlicher ist. Bei der Chrome-Untersuchung konnten wir nicht feststellen, ob der Dienst ohne große Risiken genutzt werden kann.

The screenshot shows the Google Admin console interface. The search bar contains 'Nach Nutzern, Gruppen oder Einstellungen suchen'. The breadcrumb trail is 'Apps > Zusätzliche Google-Dienste > Einstellungen für Google Play > Dienststatus'. The main content area shows the 'Google Play' settings. A message states: 'Einstellungen werden angezeigt für Nutzer in alle Organisationseinheiten'. Below this, the 'Dienststatus' is set to 'Für alle deaktiviert'. A note indicates: 'Die meisten Änderungen werden innerhalb weniger Minuten wirksam. Weitere Informationen'.

Deaktivieren Sie die personalisierte Werbung. Für K-12 ist das der Standardwert

Die K-12-Einstellung muss für alle Grund- und weiterführenden Schulen aktiviert sein.

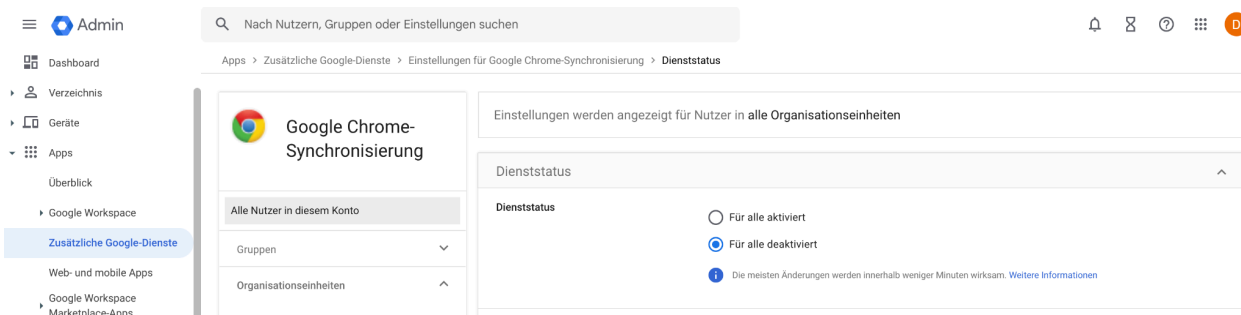
Nicht-K-12-Schulen befolgen die hier beschriebenen Anweisungen

<https://support.google.com/a/answer/6304811?hl=en>

Deaktivieren Sie die Chrome-Sync

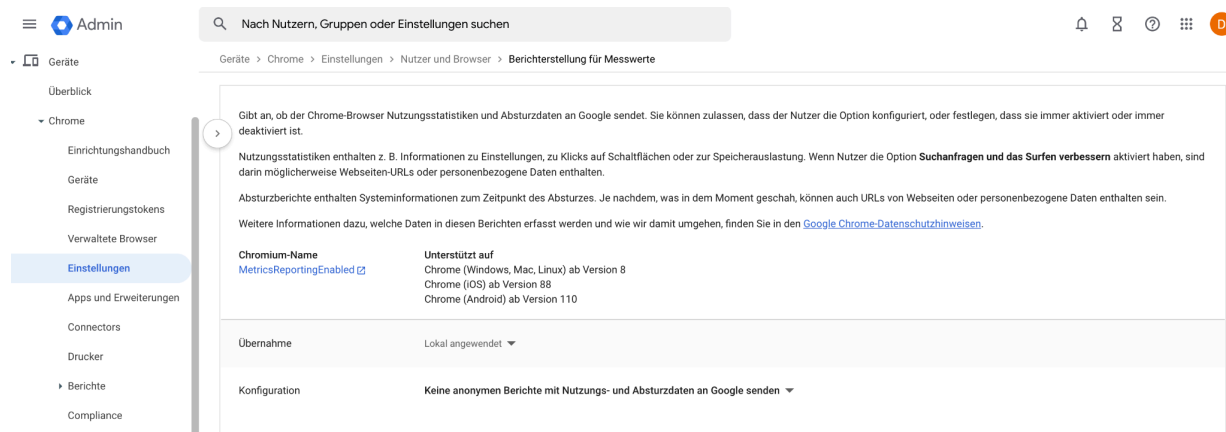
Bei der Nutzung von Chrome Sync können sensible Daten verarbeitet werden. Es gibt drei Möglichkeiten, Datenschutzrisiken zu mindern:

1. Deaktivieren Sie die Chrome-Sync (Synchronisierung)
2. Verwendet die Chrome-Sync-Verschlüsselung (der Benutzer muss dies selbst einrichten)
3. Warten Sie auf die Veröffentlichung der clientseitigen Verschlüsselung von Chrome Sync



Senden Sie keinen „Absturzbericht“ an Google

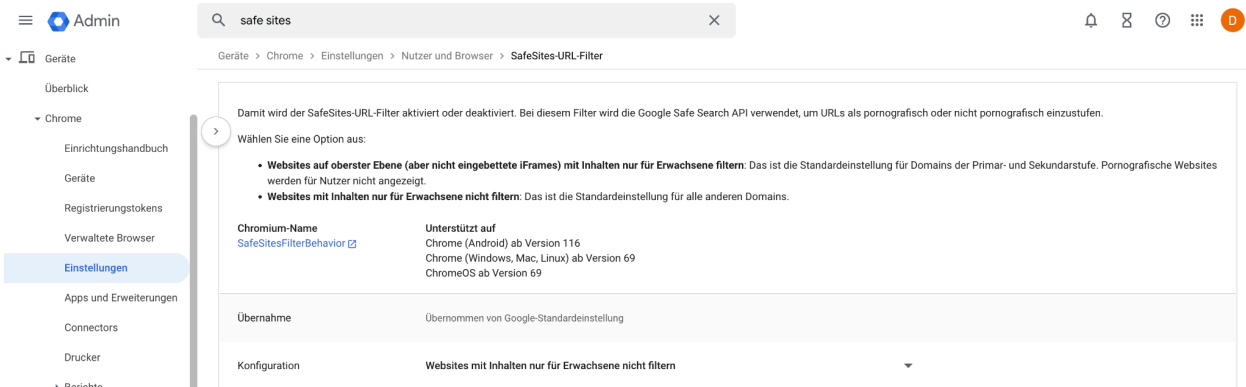
Verwenden Sie unter **Geräte -> Chrome -> Einstellungen -> Benutzer und Browser** die Einstellung „Keine Crash-Berichte senden“ an Google.



Erwägen Sie, „Safe Sites“ zu deaktivieren und eine andere Filterfunktion zu implementieren

Safe Sites ist ein wichtiger Dienst und fällt daher unter die Verarbeitungsvereinbarung. Nach Angaben von Google werden bei der Überprüfung von URLs durch Safe Sites keine Daten gespeichert. "Google erklärte, dass es keine persönlichen Identifikatoren mit den URLs sammelt und die URLs nicht speichert. Wir konnten dies nicht nachprüfen. Es besteht hier ein mögliches Risiko.

Sie können den SafeSites-URL-Filter unter Geräte -> Chrome -> Einstellungen -> Benutzer und Browser deaktivieren. Implementieren Sie dann eine weitere Filterfunktion, um den Zugriff auf Inhalte für Erwachsene zu blockieren.



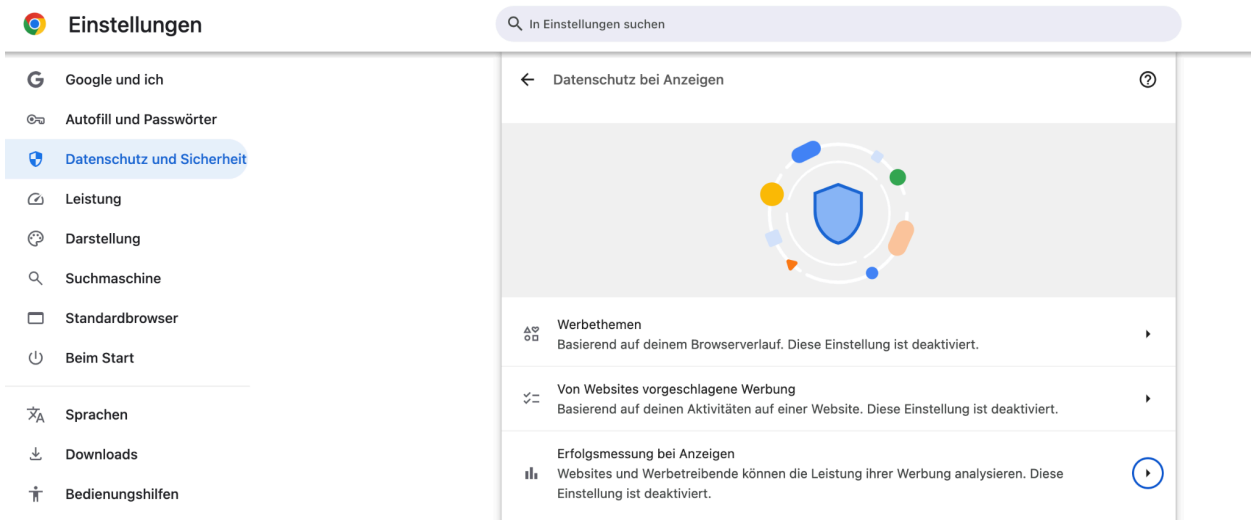
5 Endbenutzer Institutionen

Es handelt sich hier um Einstellungen, die der Endanwender selbst umsetzen muss.

Schalten Sie die Privacy Sandbox aus.

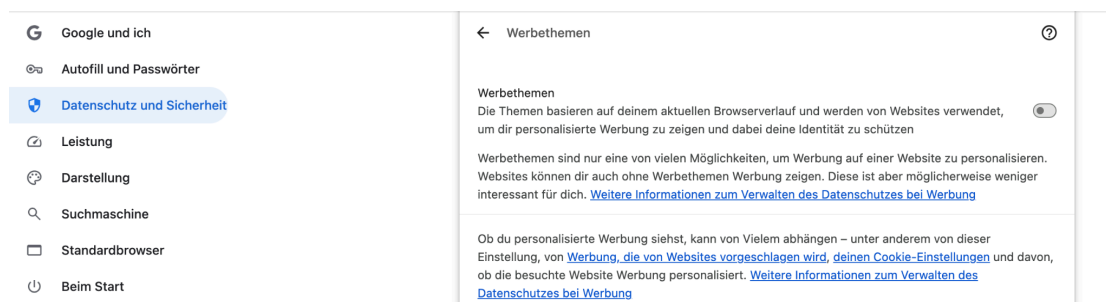
Die Privacy Sandbox ist eine neue Entwicklung zur Darstellung personalisierter Anzeigen, ohne dass Cookies von Dritten gesetzt werden. Google wird die Privacy Sandbox nicht für Nutzer testen, die unter die K-12-Einstellung fallen. Für Nutzer, die in Workspace als über 18 Jahre markiert sind, kann die Privacy Sandbox wie unten beschrieben lokal deaktiviert werden.

Gehen Sie im Browser zu **Einstellungen -> Datenschutz und Sicherheit -> Datenschutz bei Anzeigen** (ehemals Privacy Sandbox).



Jede Funktion kann separat ein- und ausgeschaltet werden.

Werbethemen deaktivieren



Von Websites vorgeschlagene Werbung abschalten

Einstellungen In Einstellungen suchen

- Google und ich
- Autofill und Passwörter
- Datenschutz und Sicherheit**
- Leistung
- Darstellung
- Suchmaschine
- Standardbrowser
- Beim Start
- Sprachen
- Downloads
- Bedienungshilfen
- System
- Einstellungen zurücksetzen

Von Websites vorgeschlagene Werbung

Von Websites vorgeschlagene Werbung

Websites, die du besuchst, können feststellen, was dir gefällt, und dir dann Werbung vorschlagen, wenn du hinterher im Internet surfst

Von Websites vorgeschlagene Werbung ist nur eine von vielen Möglichkeiten, um Werbung auf einer Website zu personalisieren. Websites können dir auch ohne diese Funktion Werbung zeigen. Diese ist aber möglicherweise weniger interessant für dich.

Websites
Du kannst unerwünschte Websites blockieren. Außerdem werden Websites, die länger als 30 Tage gelistet sind, von Chrome automatisch aus der Liste gelöscht. [Weitere Informationen](#)

Wenn diese Option aktiviert ist, wird hier eine Liste der von dir besuchten Websites angezeigt, die deine Interessen ermitteln

Von dir blockierte Websites

Ob du personalisierte Werbung siehst, kann von Vielem abhängen – unter anderem von dieser Einstellung, [den Werbethemen](#), [deinen Cookie-Einstellungen](#) und davon, ob die besuchte Website Werbung personalisiert. [Weitere Informationen zum Verwalten des Datenschutzes bei Werbung](#)

Erfolgsmessung bei Anzeigen deaktivieren

Einstellungen In Einstellungen suchen

- Google und ich
- Autofill und Passwörter
- Datenschutz und Sicherheit**
- Leistung
- Darstellung
- Suchmaschine
- Standardbrowser
- Beim Start
- Sprachen
- Downloads
- Bedienungshilfen

Erfolgsmessung bei Anzeigen

Erfolgsmessung bei Anzeigen

Websites und Werbetreibende können die Leistung ihrer Werbung analysieren

Wenn aktiviert

- Nur manche Datentypen werden zwischen Websites geteilt, um die Leistung ihrer Werbeanzeigen zu messen, wie z. B. ob du nach dem Besuch einer Website etwas gekauft hast
- Daten zur Erfolgsmessung bei Anzeigen werden regelmäßig von deinem Gerät gelöscht
- Dein Browserverlauf wird sicher auf deinem Gerät gespeichert und Berichte werden mit einer Verzögerung gesendet, um deine Identität zu schützen

Wichtige Punkte

- Du kannst jederzeit Daten zur Erfolgsmessung bei Anzeigen löschen, indem du deine Browserdaten löschst
- Chrome beschränkt die Gesamtmenge an Daten, die Websites über den Browser zur Analyse der Werbeleistung teilen können

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](#)

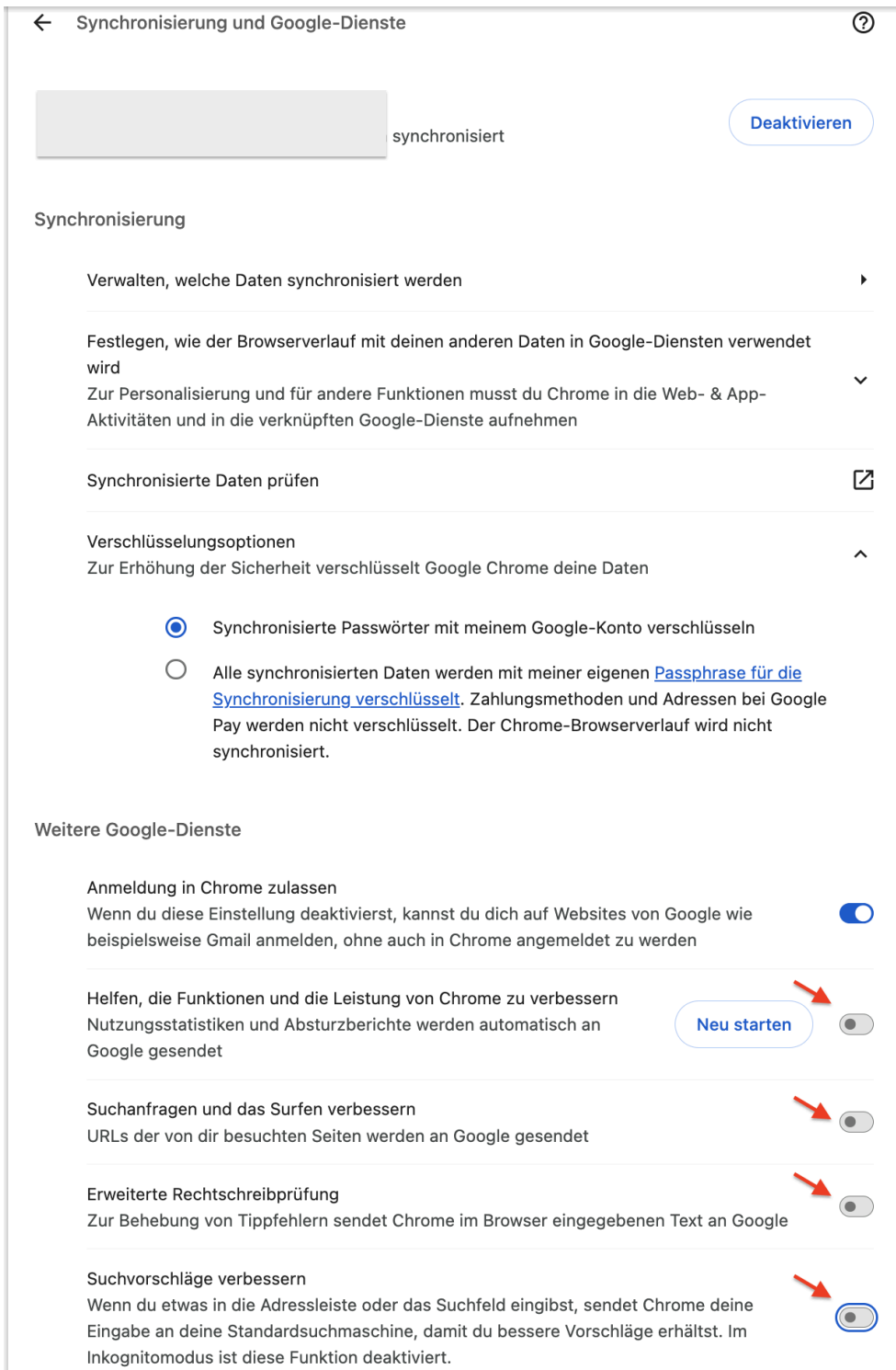
- Browsergebaseerde advertentiepersonalisatie**
Je browsegeschiedenis heeft invloed op de advertenties die je ziet
- Advertentiemeting**
Adverteerders kunnen inzicht krijgen in hoe advertenties presteren
- Spam- en fraudebeperking**
Help sites fraude te bestrijden en bots te onderscheiden van mensen

Verwenden Sie die Chrome-Sync-Verschlüsselung

The screenshot shows the Chrome Settings app on a mobile device. The left sidebar lists various settings categories, with 'Google und ich' selected. The main content area is titled 'Synchronisierung und Google-Dienste'. At the top, there is a toggle for 'Synchronisierung' which is currently turned on, with a 'Deaktivieren' button. Below this, there are sections for 'Synchronisierung', 'Verwalten, welche Daten synchronisiert werden', 'Festlegen, wie der Browserverlauf mit deinen anderen Daten in Google-Diensten verwendet wird', 'Synchronisierte Daten prüfen', and 'Verschlüsselungsoptionen'. The 'Verschlüsselungsoptionen' section has two radio button options: 'Synchronisierte Passwörter mit meinem Google-Konto verschlüsseln' (selected) and 'Alle synchronisierten Daten werden mit meiner eigenen Passphrase für die Synchronisierung verschlüsselt...'.

6 Nutzen Sie datenschutzfreundliche Browsereinstellungen

Wir empfehlen außerdem die Verwendung der folgenden datenschutzfreundlichen Browsereinstellungen.



'Do not track' deaktiviert (nicht verfolgen) und Website-Preloading deaktiviert

Wenn Sie auf Computern oder Android-Geräten im Internet surfen, können Sie eine Anfrage an Websites senden, Ihre Browserdaten nicht zu erfassen oder zu verfolgen. Diese Funktion ist standardmäßig deaktiviert.

1. Öffnen Sie Chrome auf Ihrem Computer.
2. Klicken Sie oben rechts auf Mehr \vdots > **Einstellungen**.
3. Klicken Sie auf **Privatsphäre und Sicherheit** > **Cookies und andere Websitedaten**.
4. Aktivieren oder deaktivieren Sie **Senden eine Do-Not-Track-Anfrage** mit Ihrem Browser-Verkehr.

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

Cookies en andere Websitedaten

- 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.

Datenschutz und Sicherheit

- Google und ich
- Autofill und Passwörter
- Datenschutz und Sicherheit**
- Leistung
- Darstellung
- Suchmaschine
- Standardbrowser
- Beim Start
- Sprachen
- Downloads
- Bedienungshilfen
- System
- Einstellungen zurücksetzen
- Erweiterungen
- Über Google Chrome

Hier kannst du festlegen, welche Arten von Informationen Websites verwenden können, um deine Aktivitäten während des Surfens zu erfassen.

- Drittanbieter-Cookies zulassen
- Drittanbieter-Cookies im Inkognitomodus blockieren
- Drittanbieter-Cookies blockieren**
 - Websites können Cookies verwenden, um dir das Surfen zu erleichtern; zum Beispiel, damit du angemeldet bleibst oder Artikel in deinem Einkaufswagen gespeichert bleiben
 - Websites können deine Cookies nicht verwenden, um deine Browseraktivitäten auf anderen Websites zu sehen und beispielsweise zur Personalisierung von Werbung zu nutzen. Einige Websites funktionieren dann möglicherweise nicht mehr richtig.

Ähnliche Websites dürfen meine Aktivitäten in der Gruppe sehen
Ein Unternehmen kann eine Gruppe von Websites festlegen, die deine Aktivitäten in der Gruppe mithilfe von Cookies teilen. Im Inkognitomodus ist diese Funktion deaktiviert.

Erweitert

- Bei Browserzugriffen eine „Do Not Track“-Anforderung mitsenden**
Bei dieser Anfrage ändern Websites ihr Verhalten nicht immer

Alle Websitedaten und -berechtigungen ansehen ▶

Websites, die Drittanbieter-Cookies verwenden dürfen

Dies betrifft die hier aufgeführten Websites. Wenn du „[*]“ vor einem Domainnamen einfügst, wird eine Ausnahme für die gesamte Domain erstellt. Wenn du beispielsweise „[*].google.com“ hinzufügst, können Drittanbieter-Cookies auch für „mail.google.com“ aktiv sein, da diese Subdomain zu „google.com“ gehört. Hinzufügen

Keine Websites hinzugefügt

Colophon

Handbuch für Google ChromeOS und Chrome-Browser

Datum der Ausstellung

3. Juli 2023 (Version 1.0)

27. Februar 2024 (Version 2.0)

Autoren

Version 1.0: Hans-Peter Ligthart (SIVON), Job Vos (SIVON)

Version 2.0: Hans-Peter Ligthart (SIVON)

Einige Rechte vorbehalten

Obwohl bei der Erstellung dieser Veröffentlichung größte Sorgfalt angewendet wurde, übernehmen der/die Autor(en), Herausgeber und Herausgeber von SIVON keine Haftung für etwaige Fehler oder Auslassungen. Dieses Handbuch hilft Schulbehörden als Verantwortlichen dabei, die erforderlichen Datenschutzeinstellungen in Google Chrome zu implementieren. Wenden Sie sich im Zweifelsfall an einen auf Datenschutz spezialisierten Fachanwalt, Anwalt oder Anwalt für die Anwendung in Ihrer eigenen Organisation.

Diese Publikation wurde in Zusammenarbeit mit SURF erstellt.

SIVON unterstützt Schulen dabei, eine sichere und zukunftssichere digitale Bildung jetzt und in Zukunft zu realisieren und weiterzuentwickeln; Sie berät, unterstützt und fördert die Interessen der Schulen, damit diese sich auf ihre Hauptaufgabe konzentrieren können: die bestmögliche Bildung.

Lizenz und Urheberrecht

Creative Commons Namensnennung – Nicht kommerziell – Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-NC-SA 4.0)



sivon.nl

Übersetzt und bearbeitet von datenschutz-schule.info