Google-Handbuch ChromeOS und Chrome Browser

Version 2.0 Februar 2024

Inhaltsverzeichnis

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

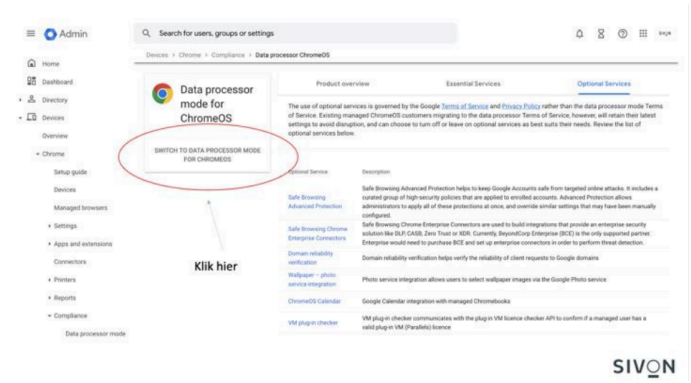
Im Mai 2023 einigten sich SURF und SIVON mit Google auf die neuen Nutzungsbedingungen (Terms of Service; ToS) für die Nutzung von ChromeOS und Chrome-Browser für Chromebooks. Sobald Sie als Schulleitung diese Vereinbarung akzeptiert und die Kontrolle über die Chromebooks übernommen haben, ist Google 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 Chrome[1] (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.

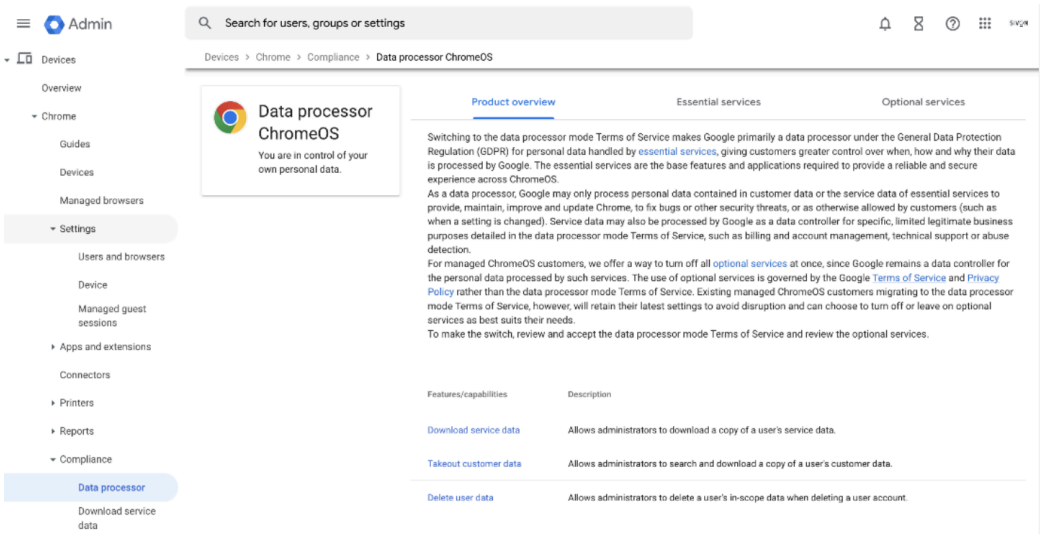
Die Standardeinstellung ist, dass Chrome OS Software-Updates automatisch durchführt. Behalten Sie diese Einstellung bei.

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



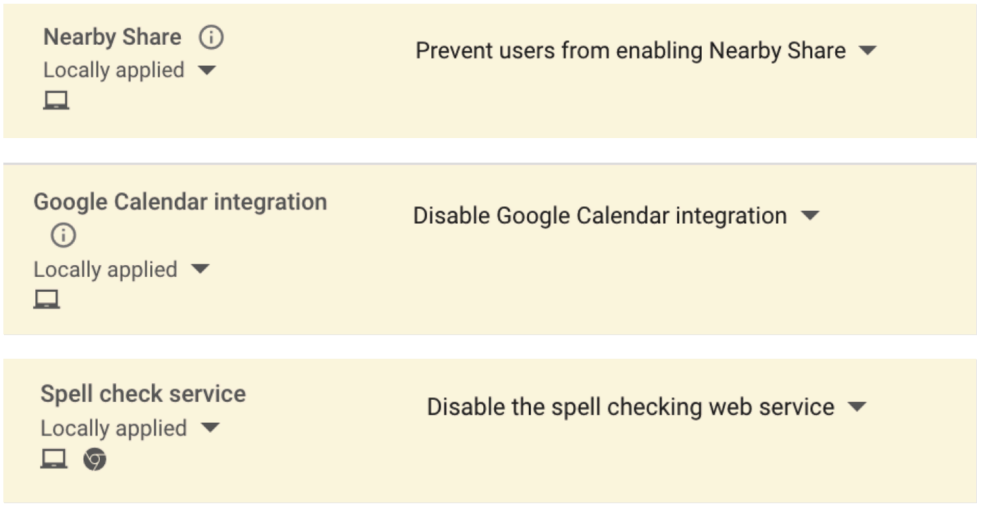
Auf dieser Seite werden die wichtigen Dienste (essential services) aufgeführt, die unter die neue Vereinbarung mit Google fallen und bei denen Google als Auftragsverarbeiter fungiert.

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.



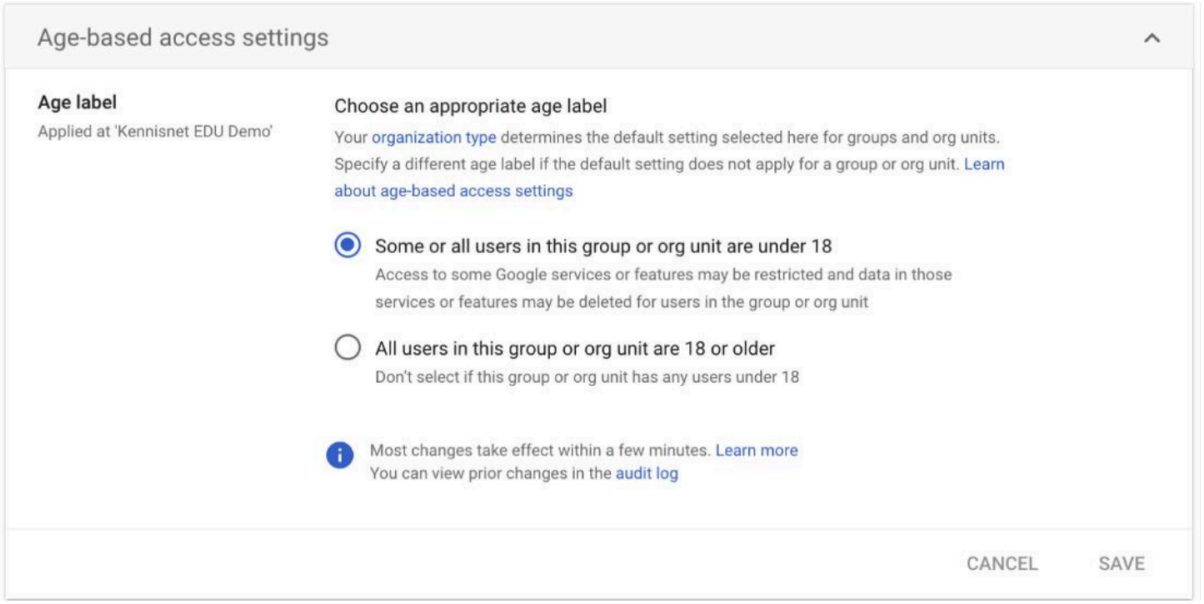
Es gibt auch einen “Haupt-Schalter“. Dies gilt nur für neue Tenants. Mit diesem Schalter können alle optionalen Dienste auf einmal ausgeschaltet werden. ACHTUNG! Wird ein optionaler Dienst bereits genutzt, kann die Nutzung des Haupt-Schalters zu Funktions- oder Datenverlusten führen.

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.

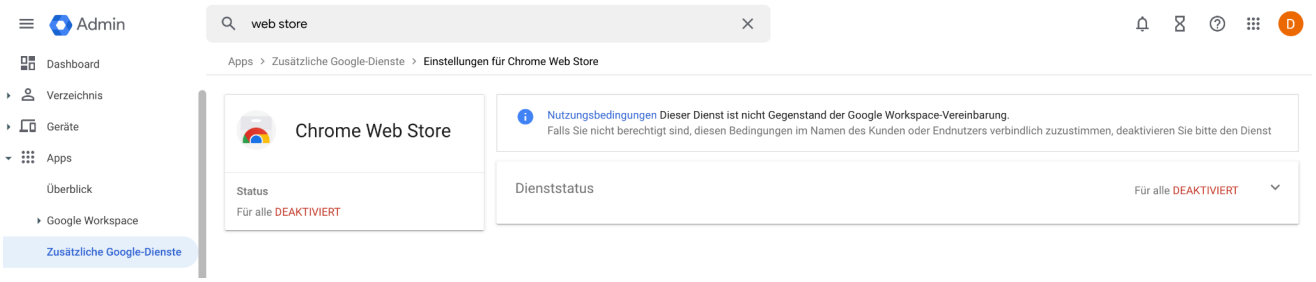
Mit der K-12-Einstellung schützen Sie Ihre Organisation vor Experimenten mit einer neuen Technologie namens Privacy Sandbox. Privacy Sandbox ist eine Möglichkeit, personalisierte Anzeigen zu schalten, ohne Cookies von Drittanbietern zu verwenden. Google sagt, dass es keine Versuche mit Privacy Sandbox 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**



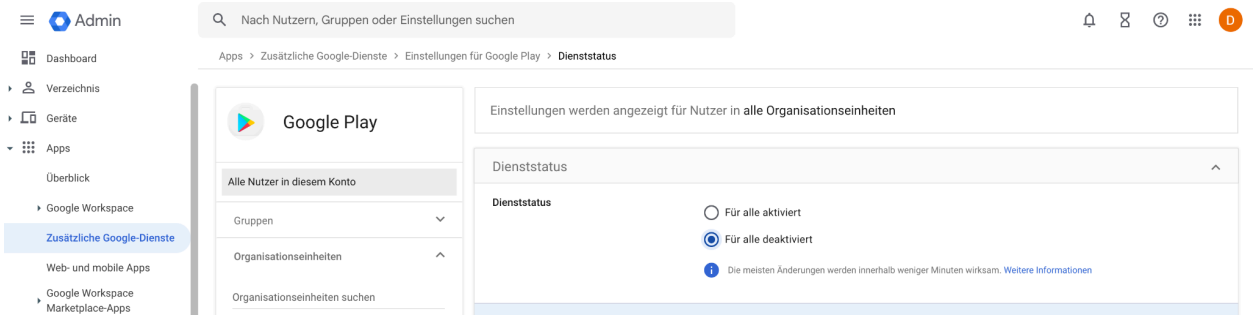
Deaktivieren Sie den Chrome Web Store

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



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

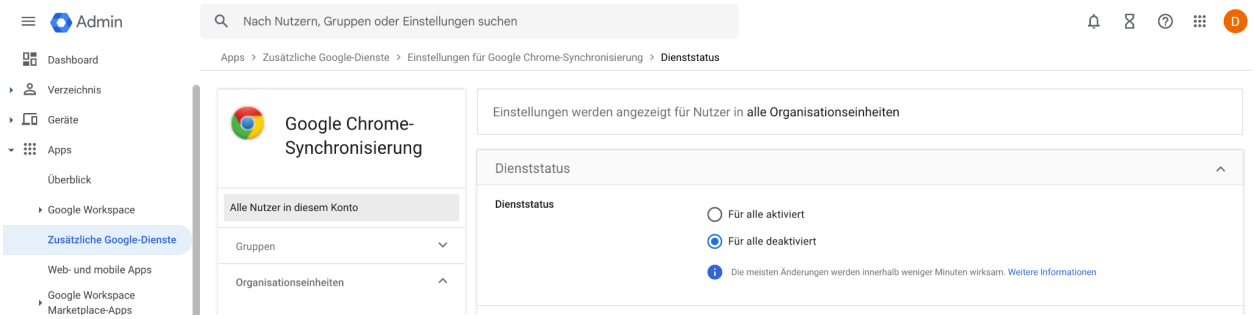
Die K-12-Einstellung muss für alle Grund- und weiterführenden Schulen aktiviert sein.

Nicht-K-12-Schulen befolgen die hier beschriebenen Anweisungen
https://support.google.com/a/answer/6304811?hl=en

Deaktivieren Sie die Chrome-Sync

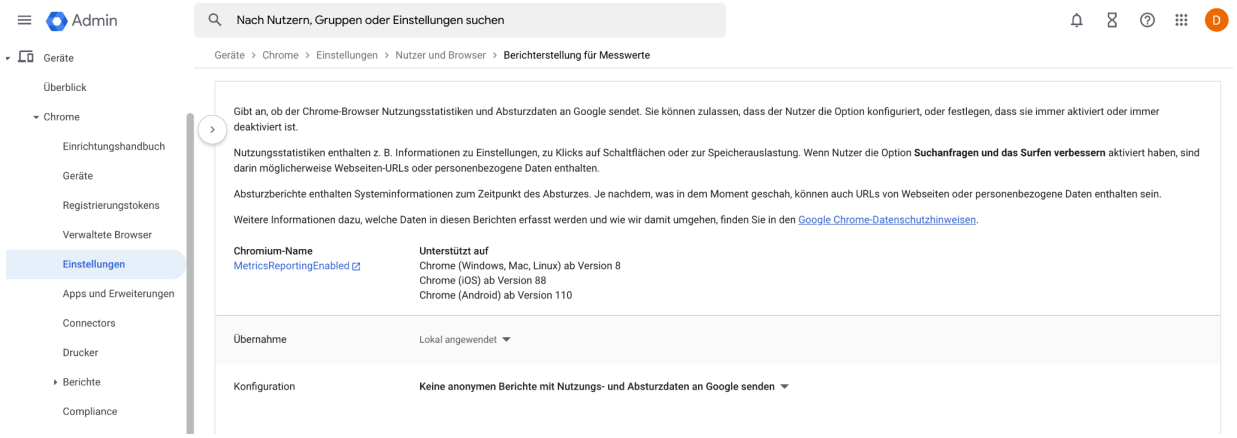
Bei der Nutzung von Chrome Sync können sensible Daten verarbeitet werden. Es gibt drei Möglichkeiten, Datenschutzrisiken zu mindern:

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

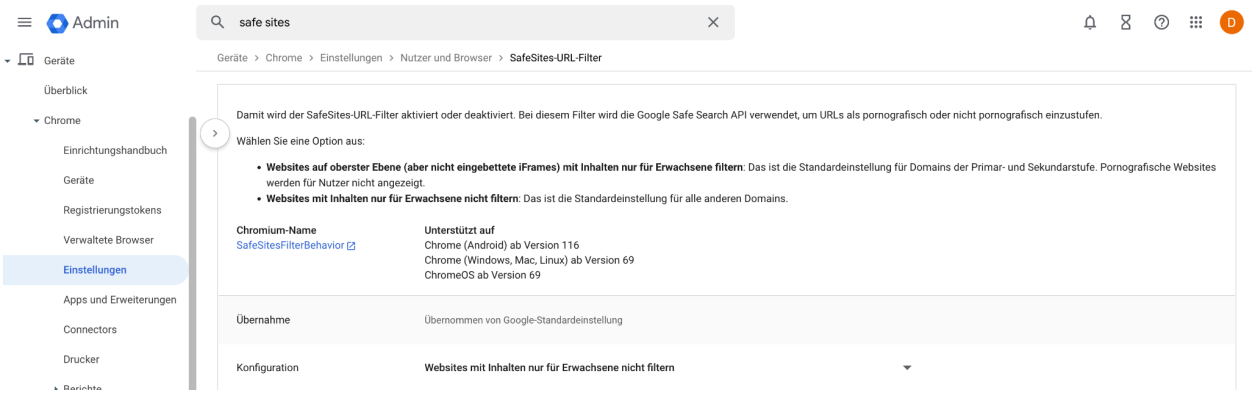
Verwenden Sie unter **Geräte -> Chrome -> Einstellungen -> Benutzer und Browser** die Einstellung „**Keine Crash-Berichte senden**“ an Google.



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.



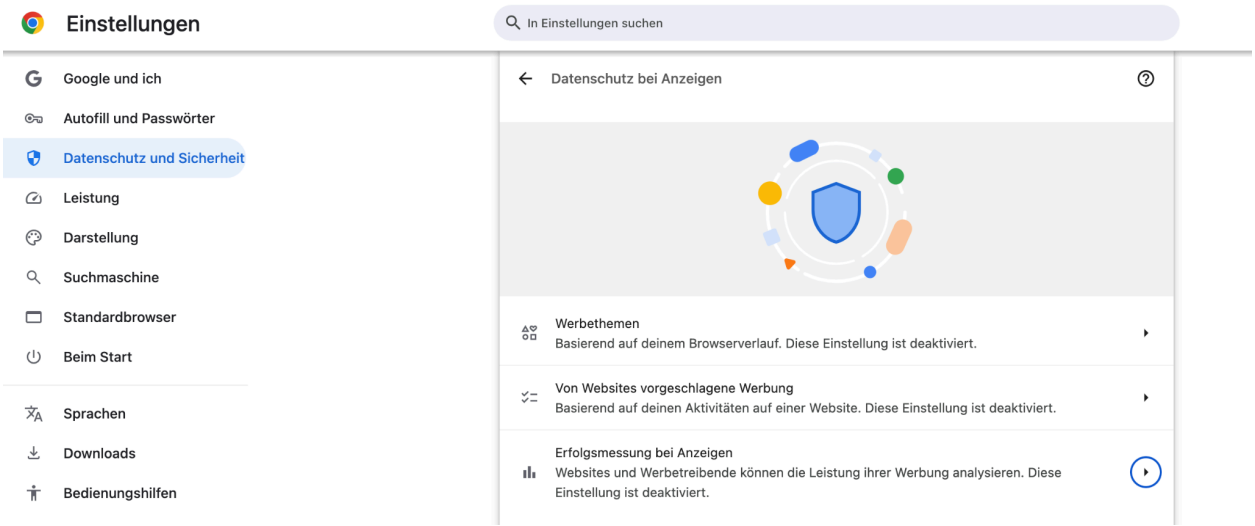
5 Endbenutzer Institutionen

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

Schalten Sie die Privacy Sandbox aus.

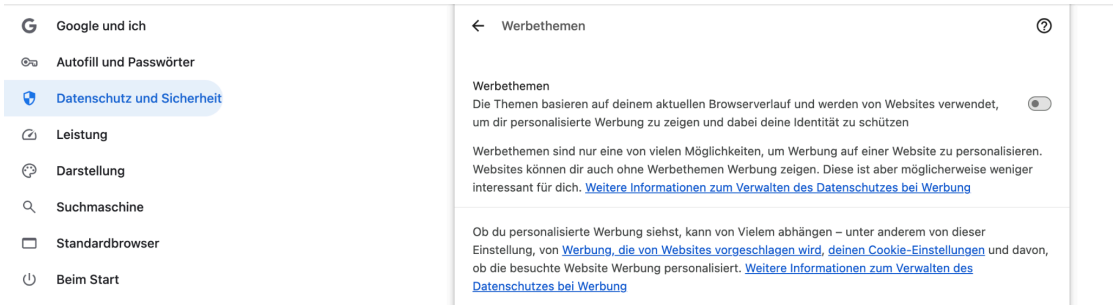
Die Privacy Sandbox ist eine neue Entwicklung zur Darstellung personalisierter Anzeigen, ohne dass Cookies von Dritten gesetzt werden. Google wird die Privacy Sandbox nicht für Nutzer testen, die unter die K-12-Einstellung fallen. Für Nutzer, die in Workspace als über 18 Jahre markiert sind, kann die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

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

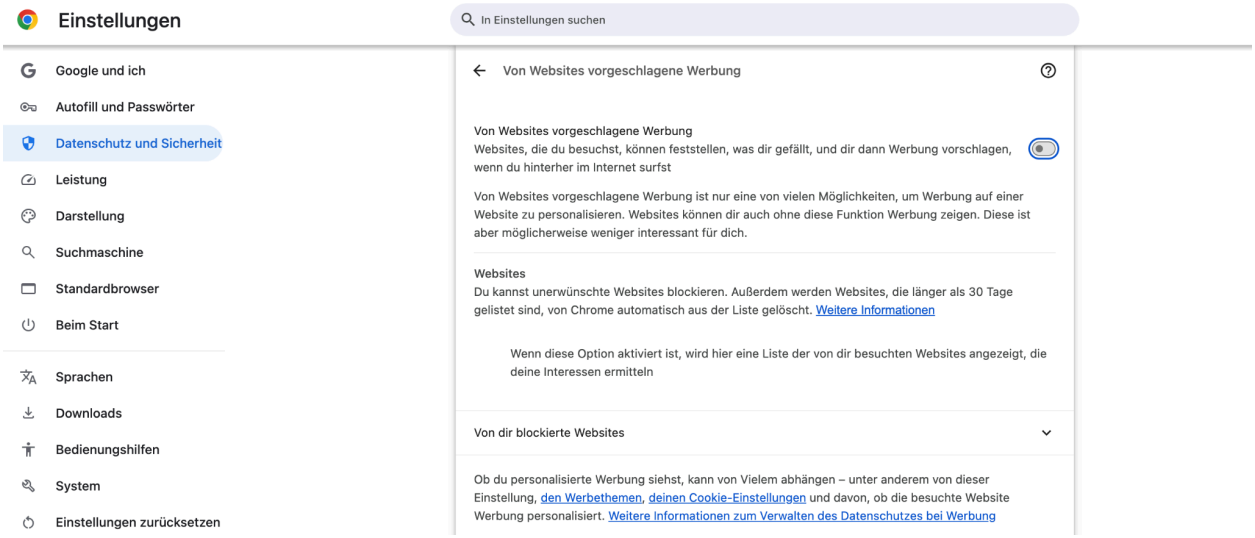


Jede Funktion kann separat ein- und ausgeschaltet werden.

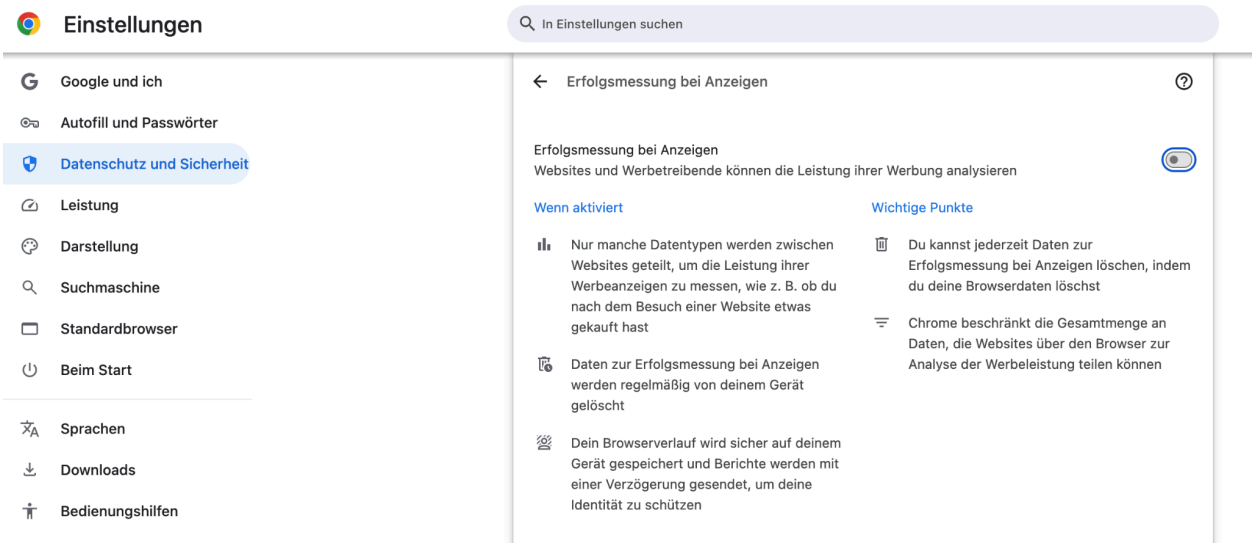
Werbethemen deaktivieren

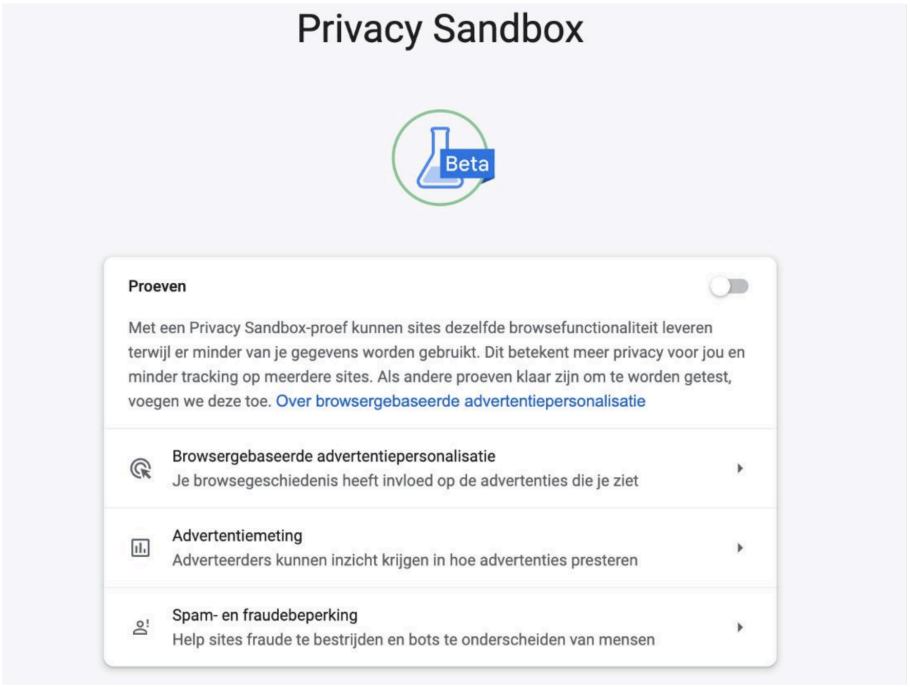


Von Websites vorgeschlagene Werbung abschalten

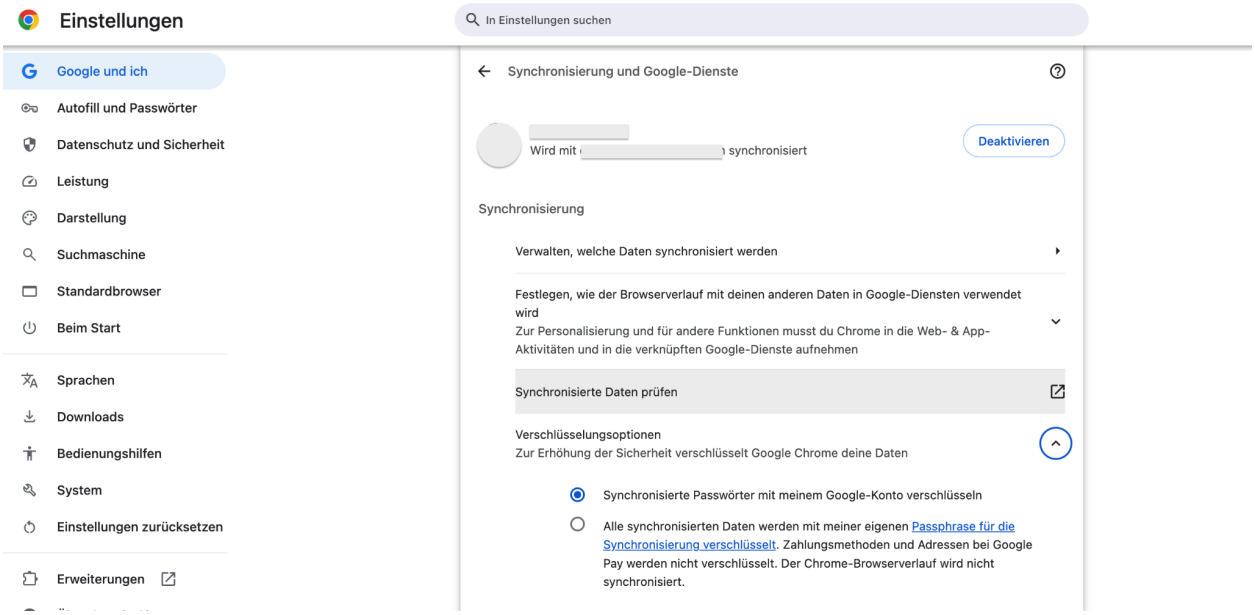


Erfolgsmessung bei Anzeigen deaktivieren



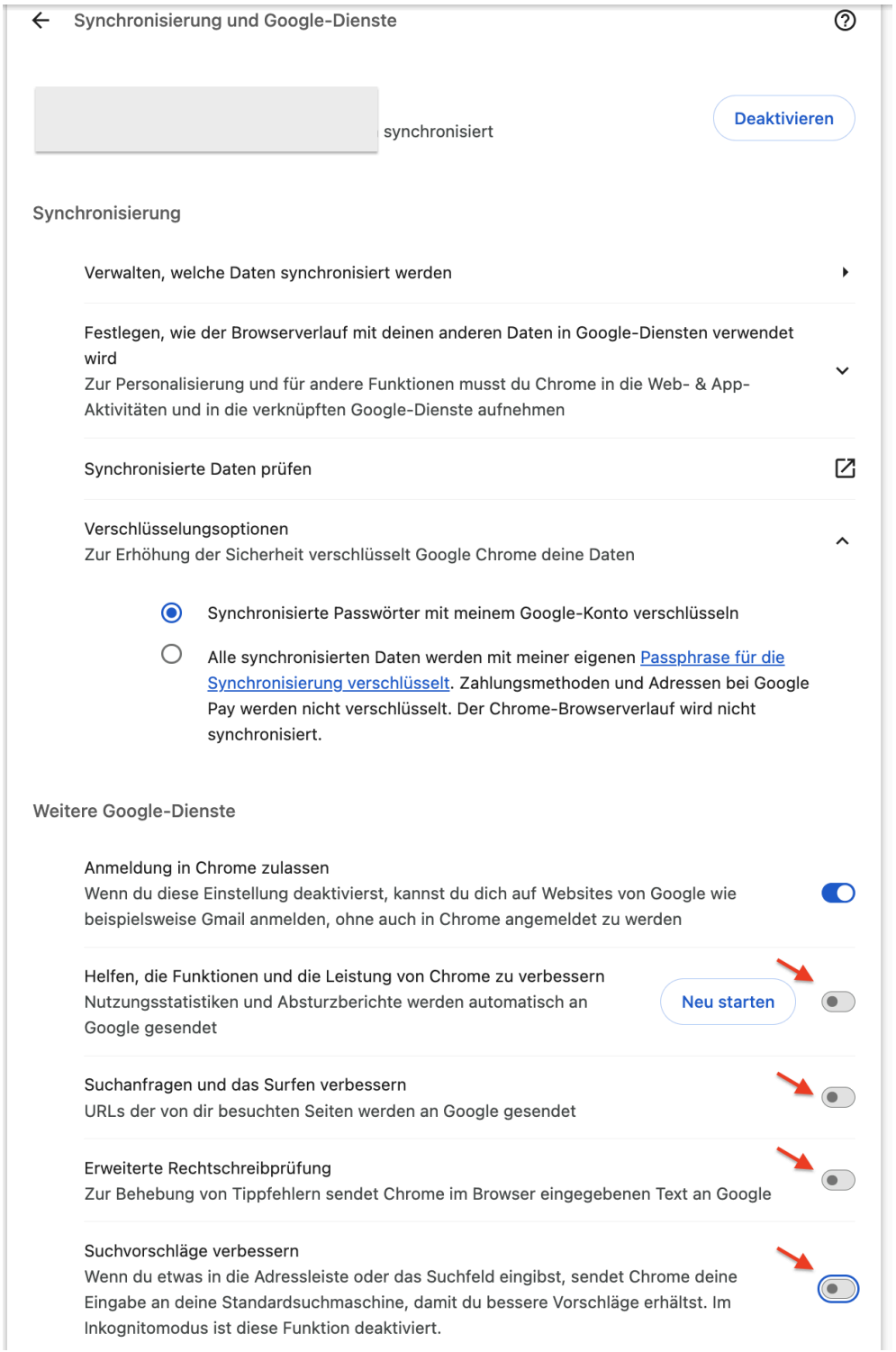


Verwenden Sie die Chrome-Sync-Verschlüsselung



6 Nutzen Sie datenschutzfreundliche Browsereinstellungen

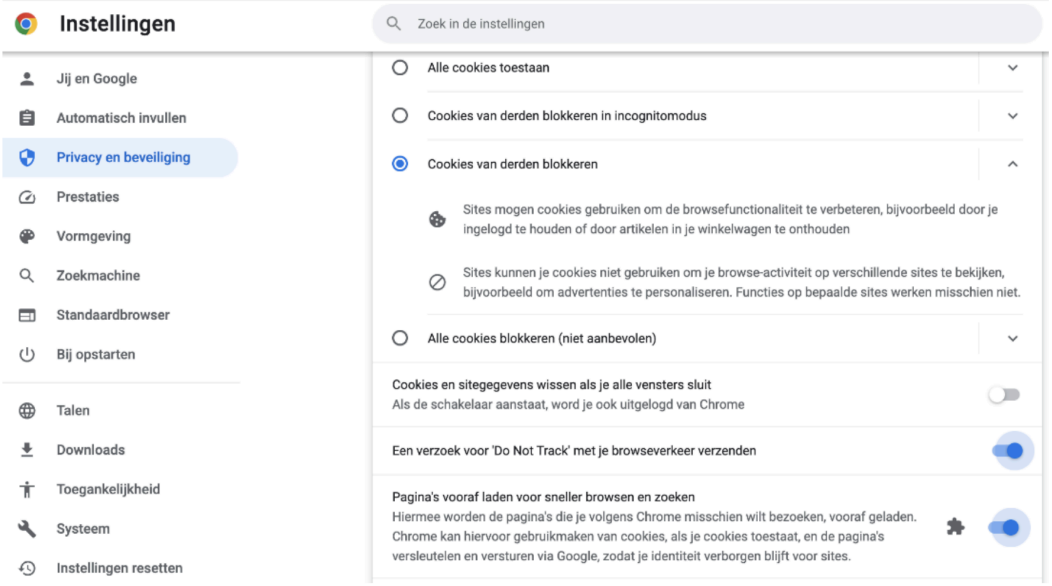
Wir empfehlen außerdem die Verwendung der folgenden datenschutzfreundlichen Browsereinstellungen.

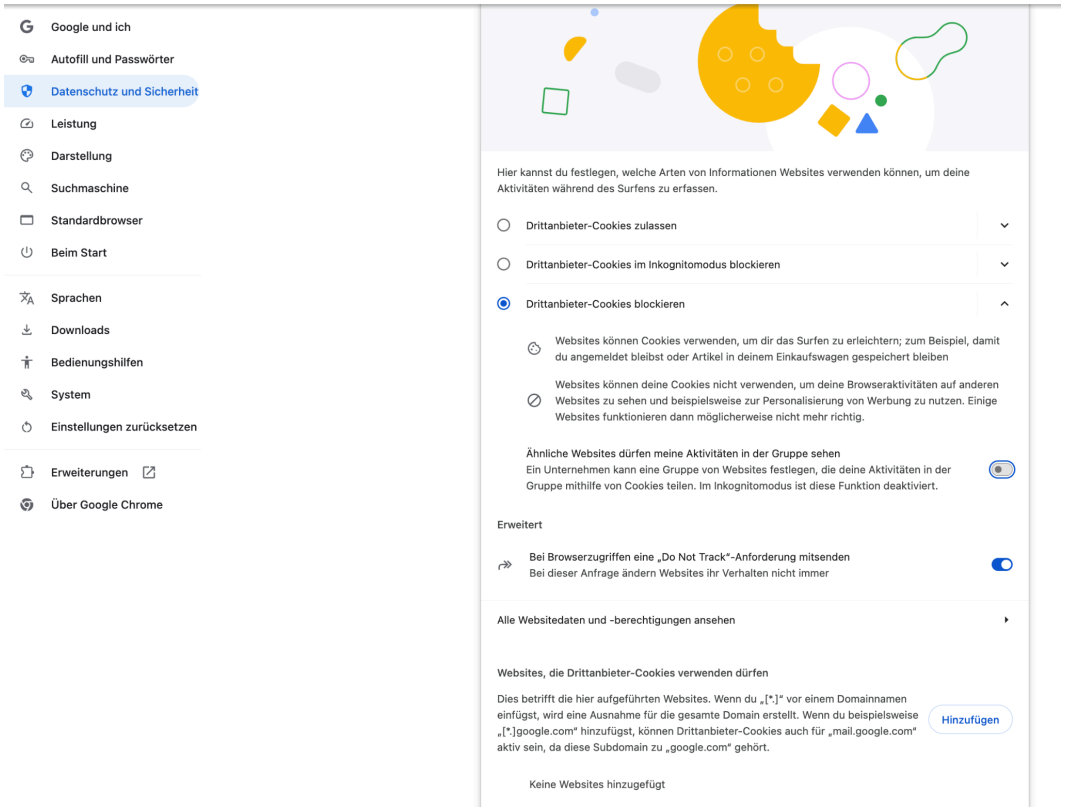


'Do not track' deaktiviert (nicht verfolgen) und Website-Preloading deaktiviert

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 ⋮ › **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.





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

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

sivon.nl

Übersetzt und bearbeitet von datenschutz-schule.info