# Technischer Leitfaden für Google Workspace for Education

Version 3.0 Februar 2024

# Inhaltsverzeichnis

| | |
|---|---|
| *2. August 2021 (Version 1.0)* | *Erste Version des technischen Handbuchs mit enthält eine Beschreibung der Google Workspace-Einstellungen, die Schulen implementieren müssen PRivacy-Risiken aus dem DPIA-Update vom August 2021 mildern.* |
| *20. Juli 2023 (Version 2.0)* | *Im Zeitraum August 2021 bis Juni 2023 Google hat verschiedene Datenschutzverbesserungen implementiert Arbeitsplatz. Trotz der Anpassungen durch Google alle Maßnahmen aus 2021 gelten weiterhin. In Version 2 des technischen Handbuchs ist jetzt verfügbar bezogen auf den aktuellen Stand der Dinge wie z nach der Verifizierung der Genome bekannt Maßnahmen von Google.*<br>*Version 2 enthält zusätzliche Informationen zu Cookies und Youtube.* |
| *31. August 2023 (Version 2.1)* | *Hinzufügung einer Versionsverwaltungstabelle und Änderungen Formatierung* |
| *27. Februar 2024 (Version 3.0)* | *Update nach DTIA* |

# 1 Einleitung

Für Workspace for Education (im Jahr 2021 G Suite for Education genannt) wurde eine Datenschutz Untersuchung durchgeführt. Diese Datenschutz-Folgenabschätzung (DSFA) ergab, dass mit der Nutzung von Google Workspace for Education hohe Datenschutzrisiken verbunden sind.

SIVON und SURF, Genossenschaften von und für Bildungs- und Forschungseinrichtungen in den Niederlanden, trafen im Jahr 2021 als Reaktion auf die Untersuchung Vereinbarungen mit Google, um die festgestellten Datenschutzrisiken zu verringern. Google erfüllte die Vereinbarung und ergriff die erforderlichen Maßnahmen und nahm Änderungen an seiner Software vor. Diese wurden Mitte 2023 von SIVON und SURF und den von ihnen beauftragten externen Datenschutzexperten überprüft. Diese Ergebnisse sind im „Verifizierungsbericht Google Abhilfemaßnahmen Workspace for Education“ der Privacy Company (Stand 15. Juni 2023) enthalten.

Zusätzlich zu den von Google vorgenommenen Änderungen müssen Bildungseinrichtungen selbst Maßnahmen ergreifen, um die Risiken zu mindern. Dazu gehören Einstellungen, die Administratoren (Admins) in Google Workspace for Education ändern können, sowie Änderungen, die Nutzer selbst vornehmen können.

Sie umfasst auch Maßnahmen, die auf die Nutzung von Chrome-Geräten und des Chrome-Browsers abzielen. Im Jahr 2023 wird die Datenschutzstudie zu Chrome abgeschlossen sein. Nach dieser Untersuchung wurden zusätzliche Maßnahmen beschrieben.

Schließlich wurde eine DTIA zu Google Workspace for Education (Google meet) im Jahr 2023 durchgeführt. Eine DTIA identifiziert die Risiken der internationalen Übertragung. Das Risiko des internationalen Transfers wurde ab 2021 in die DTIA aufgenommen, nachdem das Schrems-II-Urteil das EU-US-Privacy Shield für ungültig erklärt hatte. In der DPIA ist dies das Risiko 9. Version 3.0 dieses Handbuchs beschreibt die Maßnahmen, die zu ergreifen sind, um die Risiken des internationalen Transfers zu mindern. Die Maßnahmen sind in Kapitel 7 beschrieben.

Alle in diesem Leitfaden aufgeführten Aktionen sind Maßnahmen zur Verbesserung des Datenschutzes, die bei der Minderung der Risiken der Verwendung von Workspace for Education (Plus) im Bildungswesen berücksichtigt wurden. Wenn eine Bildungseinrichtung beschließt, eine oder mehrere der Maßnahmen nicht zu implementieren, wirkt sich dies auf die Betrachtung der Datenschutzrisiken aus. Die Bildungseinrichtung muss dann selbst nachweisen, dass die Nichtdurchführung der technischen Maßnahme keine Auswirkungen auf die Datenschutzrisiken hat und/oder welche Ausgleichsmaßnahmen die Bildungseinrichtung ergreift, um sicherzustellen, dass das Datenschutzrisiko bei der Nutzung von Workspace for

Education nicht steigt. Die Nichteinhaltung der technischen Maßnahmen ist daher nicht ohne Folgen und muss vom Datenschutzbeauftragten ausdrücklich beschrieben und geprüft werden.

Mehrere Produkte oder Funktionen von Google Workspace for Education geben (potenziell) datenschutzrelevante Daten an Google weiter. In diesem Leitfaden wird erläutert, wie Sie die Datenmenge minimieren können, indem Sie die Einstellungen für Nutzerkonten und Produkte anpassen. Wir erklären, welche Maßnahmen Sie ergreifen müssen, warum dies notwendig ist und wie Sie sie umsetzen.

Dieser Leitfaden ist Teil von drei Schritten, die Schulen selbst durchführen müssen, bevor sie Google Workspace for Education (weiterhin) nutzen können:

1. Akzeptieren Sie die geänderten Bedingungen der Bildungsvereinbarung Workspace for Education.
2. Gehen Sie diese technischen Schritte durch und setzen Sie sie um.
3. Durchführung von bildungsspezifischen DPIA (auf der Grundlage des lokalen DPIA-Handbuchs von SURF, SIVON und Kennisnet).

# 2 Allgemeine Hinweise und Informationen

## 2.1 Information des Personals, der Schüler, Studenten und ihrer Eltern

Es empfiehlt sich, Ihre Mitarbeiter, Schüler, Studenten und deren Eltern zu Beginn des Schuljahres über die Nutzung von Google Workspace for Education und die gewählten Datenschutzeinstellungen zu informieren. SIVON stellt zu diesem Zweck Musterbriefe für Mitarbeiter und Eltern zur Verfügung. Diese enthalten insbesondere Informationen über die Datenverarbeitung durch Google, die Vereinbarungen der Bildungseinrichtung mit Google und "hochrangige Informationen" über die Risiken der Nutzung von Workspace for Education. Letzteres bedeutet, dass die Vereinbarungen mit Google nur gelten, solange Mitarbeiter, Schüler und Studenten in ihren Konten angemeldet sind und nicht mit einem privaten Konto bei Google. Es ist wichtig, Schüler und Studenten daran zu erinnern, dass, wenn ihr Profilbild aus ihrem Konto verschwindet, dies bedeutet, dass sie die geschützte Workspace for Education-Umgebung verlassen haben.

Darüber hinaus wird Mitarbeitern, Schülern und Studenten allgemein empfohlen, so wenig (besondere) personenbezogene Daten wie möglich in ihre Kontoinformationen und in die Informationen, die sie anderen mitteilen, aufzunehmen.

## 2.2 Auskunftsanfragen

Angestellte, Schüler und Studenten, die mehr Informationen über die Daten, die Google von und über sie verarbeitet, wünschen, können über den Administrator von Workspace for Education Informationen von ihrer Bildungseinrichtung anfordern. Wenn sich ein Mitarbeiter, Schüler oder Student darüber beschwert, dass die Antwort auf sein Auskunftsersuchen unvollständig ist, beruft sich Google auf die Ausnahme des AVG, wonach keine Auskunft erteilt wird, wenn die betroffene Person nicht identifiziert werden kann. Nur die Bildungseinrichtung und nicht Google kann die Nutzer identifizieren. In Ermangelung einer

Identifizierung der Nutzer behauptet Google, dass es nicht berechtigt ist, Informationen über die betroffenen Personen zu liefern.

## 2.3 Übermittlung personenbezogener Daten in Drittländer

Bis 2023 ist die Datenübermittlungs-Folgenabschätzung (DTIA) abgeschlossen, wie in den Stellungnahmen der Datenschutzaufsichtsbehörde (AP) und des EDPB beschrieben. Akzeptieren Sie die (neuen) Standardvertragsklauseln von Google https://cloud.google.com/security/compliance/eu-scc. Die Ergebnisse der DTIA werden zur Verfügung gestellt, sobald sie von SURF und SIVON fertiggestellt sind. Weitere Informationen über die Übermittlung personenbezogener Daten finden Sie in dem Artikel Empfehlungen für die Übermittlung von Daten in  unsichere Länder final.

## 2.4 Unterauftragsverarbeiter

Eines der Risiken ist das Fehlen von Informationen über Googles Zulieferer (Unterauftragsverarbeiter).  Google setzt Unterauftragsverarbeiter für drei Arten von Tätigkeiten ein (Zweckbindung).

**Rechenzentrumsbetrieb:** Verwaltung des Google-Rechenzentrums, in dem die Kundendaten gespeichert werden.  Der Unterauftragsverarbeiter hat keinen Zugang zu den Kundendaten.

**Service-Wartung:** Unterauftragsverarbeiter für technische Wartung und Fehlerbehebung bei Software und Hardware. Der Unterauftragsverarbeiter kann begrenzten Zugang zu Kundendaten benötigen, um technische Probleme zu lösen.

**Technische Unterstützung:** Wenn eine Schulbehörde eine  Support-Anfrage stellt, wird diese an einen Unterauftragsverarbeiter weitergeleitet. Der Unterauftragsverarbeiter hat Zugang zu den Daten, die die Schulbehörde zusammen mit einer Support-Anfrage sendet.

Informationen zu den Unterauftragsverarbeitern von Google finden Sie auf dieser Seite.

## 2.5 Weitere Informationen zum Datenschutz

Weitere Informationen zum Chrome-Datenschutz finden Sie im Google Chrome Privacy Whitepaper. https://www.google.com/chrome/privacy/whitepaper.html

Weitere Informationen darüber, welche Ratschläge Google zur Einhaltung der DS-GVO gibt, finden Sie im Google Workspace Edu Data Protection Implementation Guide. https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf

## 2.6 Geltungsbereich

Die geänderten Geschäftsbedingungen Education Agreement Workspace for Education gelten nur für die sogenannten Kerndienste *Core Services* (wie Gmail, Google Calendar, Doc, Drive und Classroom). Die vollständige Liste https://workspace.google.com/intl/en/terms/user_features.html

Zusätzliche Dienste (*Additional Services)* (z. B. Youtube, Google Maps, Blogger etc.) sind nicht Gegenstand der Vereinbarung.

# 3 Überblick über die Maßnahmen

Die Bildungseinrichtung muss verschiedene Funktionalitäten von Google Workspace for Education auf bestimmte Weise einrichten oder deaktivieren. Die nachstehende Tabelle gibt einen Überblick über die von Ihnen zu ergreifenden Maßnahmen und die damit verbundenen Managementmethoden. Die Maßnahmen werden in den folgenden Kapiteln näher erläutert, einschließlich Informationen zur Umsetzung.

Die Bildungseinrichtung muss mehrere Funktionen von Google Workspace for Education auf eine bestimmte Weise einrichten oder deaktivieren. Die nachstehende Tabelle gibt einen Überblick über die zu treffenden Maßnahmen und die entsprechende Art der Verwaltung. In den folgenden Abschnitten werden die Maßnahmen ausführlicher erläutert und Informationen zur Umsetzung gegeben.

Es wurden zusätzliche Datenschutzuntersuchungen zu Chromebooks durchgeführt. Die Ergebnisse wurden am 3. Juli 2023 veröffentlicht.
https://sivon.nl/2023/07/sivon-surf-en-google-bereiken-overeenkomst-terms-of-service-google-chrome/

## 3.1 Struktur

Die Maßnahmen verteilen sich wie folgt

Für die Umsetzung der zu ergreifenden Maßnahmen gibt es drei Umsetzungswege:

- Zentrale Verwaltung von Geräten und Browsern (Geräteverwaltung)
- Zentrale Verwaltung der Einstellungen über die Google Workspace Admin-Konsole.
- Zentrale Verwaltung der Einstellungen über Gruppenrichtlinien des Betriebssystems. • Individuelle Einstellungen.

Maßnahmen, die die Datenminimierung bei der Nutzung von Produkten oder Funktionalitäten betreffen, können entweder über die Admin-Konsole oder über die Gruppenrichtlinie des Betriebssystems umgesetzt werden.

Schließlich enthält dieses Handbuch auch generische Maßnahmen. Hierbei handelt es sich um Maßnahmen, die nicht spezifisch für Google sind, aber auch allgemein nützlich sind, um Datenschutzrisiken zu begrenzen. Diese Maßnahmen sind:

- Nutzung von YouTube von anderen Plattformen aus.
- Richtlinie zu Cookies.
- Weisen Sie Benutzer auf die Verwendung datenschutzrelevanter Informationen in Datei- und Ordnernamen hin.
- In E-Mail-Adressen dürfen keine echten Namen von Mitarbeitern, Schülern oder Studenten verwendet werden.
- Installieren Sie eine Browser Erweiterung, die das Tracking blockiert.
- Benutzen Sie eine datenschutzfreundliche Suchmaschine wie DuckDuckGo oder Startpage.

## 3.2 Maßnahmen in Bezug auf Benutzerkonten

| | |
|---|---|
| **Benutzerprofil** | Richten Sie ein K-12-Profil für alle Benutzer ein |
| **Benutzerdaten** | Verwenden Sie in E-Mail-Adressen keine echten Namen von Mitarbeitern, Schülern oder Studenten |
| | Verbieten Sie Benutzern, Profile selbst anzupassen |
| **Speicherung von geografischen Standortdaten** | Google Cloud-Speicherort nach Europa ändern, wenn möglich |
| **Zusätzliche Google-Dienste** | Deaktivierung zusätzlicher Google-Dienste. Auch wenn Sie Google Workspace nicht nutzen, bestehen Datenschutzrisiken bei der Nutzung zusätzlicher Google-Dienste wie YouTube. |
| **Google Workspace Marktplatz-Apps** | Erlauben Sie Benutzern nicht, Apps vom Google Workspace Marketplace zu installieren |
| **Neue Google Produkte** | Neue Produkte werden den Benutzern nicht automatisch zur Verfügung gestellt |

## 3.3 Maßnahmen zur Datenminimierung in Produkten und Funktionalitäten

| Produkt oder Funktionalität | Einstellung der Admin-Konsole | Betriebssystem Gruppenrichtlinie |
|---|---|---|
| **Rechtschreibprüfung** | Die lokale Rechtschreibprüfung kann eingeschaltet sein | SpellCheckEnabled: true |
| **Webdienst zur Rechtschreibprüfung** | Deaktivieren Sie den Webdienst für die Rechtschreibprüfung | SpellCheckServiceEnabled: false |
| **Chromebrowser** | Chrome-Synchronisierung nicht zulassen | ClearBrowsingDataOnExit List SyncDisabled |
| **Automatische Übersetzung Websites** | Schlagen Sie niemals eine Übersetzung vor | TranslateEnabled: false |
| **Geolokalisierung** | Erlauben Sie Websites nicht, die Geolokalisierung von Benutzern zu ermitteln | DefaultGeolocationSetting: 2 |
| **Benutzer-Feedback-Formular** | Erlauben Sie kein Benutzer-Feedback | UserFeedbackAllowed: false |
| **Berichtsstatistiken** | Senden Sie niemals anonyme Benutzerberichte oder Absturzdatenberichte an Google | MetricsReportingEnabled: false |

| | | |
|---|---|---|
| **Neuer Tab Inhaltsvorschläge** | Auf der Seite „Neuer Tab“ werden keine Inhaltsvorschläge angezeigt | NTPCardsVisible: false |
| **Tab „Werbung“. Inhalt** | Deaktivieren Sie die Anzeige von Werbeinhalten im vollständigen Tab | PromotionTabsEnabled: false |
| **Neuer Tab „Karten“.** | Auf der Seite „Neuer Tab“ werden keine Karten angezeigt | NTPContentSuggestionsEnabled: false |
| **Vorgeschlagenen Dienst durchsuchen** | Erlauben Sie Benutzern niemals, Suchvorschläge zu verwenden | SearchSuggestEnabled: false |

| | | |
|---|---|---|
| **Anmeldung bei sekundären Konten** | Erlauben Sie Benutzern nur, sich mit einem Konto bei der Schuldomäne anzumelden | SecondaryGoogleAccountSignin Allowed: false |
| **Cookies** | Blockieren Sie Cookies von Drittanbietern | BlockThirdPartyCookies: true |
| **Cookies** | Speichern Sie Cookies nur für die Dauer der Sitzung | DefaultCookieSettings: |
| **Systemberichte von besuchte Seiten** | Übermittlung zusätzlicher Daten zur Verbesserung von Safe Browsing, Deaktivierung | SafeBrowsingExtendedReportin gEnabled: false |
| **Chrome-Bereinigung** | Regelmäßiges Scannen nicht zulassen oder Ergebnisse von Chrome Cleanup werden nie an Google weitergegeben | ChromeCleanupEnabled: false - OF - ChromeCleanupReportingEnabl ed: false |

## 3.4 Einzelmaßnahmen und Hinweise

| | |
|---|---|
| **Anzeigenpersonalisierung** | Individuell einstellen, wenn kein K-12-Benutzerprofil vorhanden ist. |
| **Einbettung von YouTube-Videos** | Verwenden Sie eingebettete Videos nur im „erweiterten Datenschutzmodus“. |
| **Verwenden Sie keinen Chrome Browser** | Verwenden Sie einen alternativen Browser, bis die neue Version herauskommt, bei der Google als Datenverarbeiter fungiert. |
| **Verwenden Sie Google nicht** | Verwenden Sie eine datenschutzfreundliche Suchmaschine wie |

| | |
|---|---|
| **als Suchmaschine** | DuckDuckGo oder Startpage. |
| **Verwenden Sie einen Werbe- und/oder Trackingblocker** | Installieren Sie eine Browser Erweiterung, die das Tracking blockiert. |
| **Verwenden Sie keine datenschutz sensible Informationen in Datei- und Ordnernamen** | Weisen Sie Benutzer auf datenschutzrelevante Informationen in Datei- und Ordnernamen hin |

# 4 Aktivieren Sie zentrale Verwaltungsoptionen

## 4.1 Verwaltung von Chromebooks und Chrome-Browsern

Google Workspace-Administratoren verfügen über eine Art von Konto, das eine umfassende Kontrolle über die mit Google geteilten Daten ermöglicht. Die meisten Maßnahmen können zentral über die Google Workspace Admin-Konsole verwaltet werden.

Um dies zu ermöglichen, müssen die Chromebooks und Chrome-Browser einer Organisation tatsächlich unter Verwaltung gestellt werden. Dazu müssen die Chromebooks und Chrome-Browser bei Ihrer Organisation und der entsprechenden Organisationseinheit in Google Workspace angemeldet werden.  Diese übernehmen dann alle Einstellungen, die Sie in der Google Workspace Admin-Konsole festlegen.

Bei Chromebooks muss das gesamte Gerät verwaltet werden. Für die Betriebssysteme Windows, Mac und Linux muss der Chrome-Browser unter Verwaltung gestellt werden. Nachfolgend finden Sie die Anweisungen, um dies zu erreichen.

## 4.2 Chromebooks verwalten

Die Verwaltung von Chromebooks erfolgt in der Regel über Ihren Anbieter. Für die zentralisierte Verwaltung von Chromebooks benötigen Sie die Chrome Education Upgrade-Lizenz. Wenn Ihr Anbieter Ihre Chromebooks noch nicht in die zentrale Verwaltung aufgenommen hat, gehen Sie wie folgt vor.

Wenn Sie ein neues Chromebook oder ein Chromebook starten, bei dem ein Power-Wash (Zurücksetzen auf die Werkseinstellungen) durchgeführt wurde, klicken Sie nach dem Herstellen einer WLAN-Verbindung und dem Akzeptieren der Nutzungsbedingungen auf „Für Enterprise anmelden“. Hier geben Sie die Zugangsdaten eines Benutzers mit Registrierungsrechten ein. Das Chromebook ist jetzt in Ihrer Workspace-Umgebung für die zentrale Verwaltung registriert.

In der Google Workspace-Verwaltungsumgebung können Sie dieses Chromebook nun in der gewünschten Organisationseinheit platzieren, z. B. im Klassenzimmer.

## 4.3 Von Chromebooks verwaltete Gastsitzung

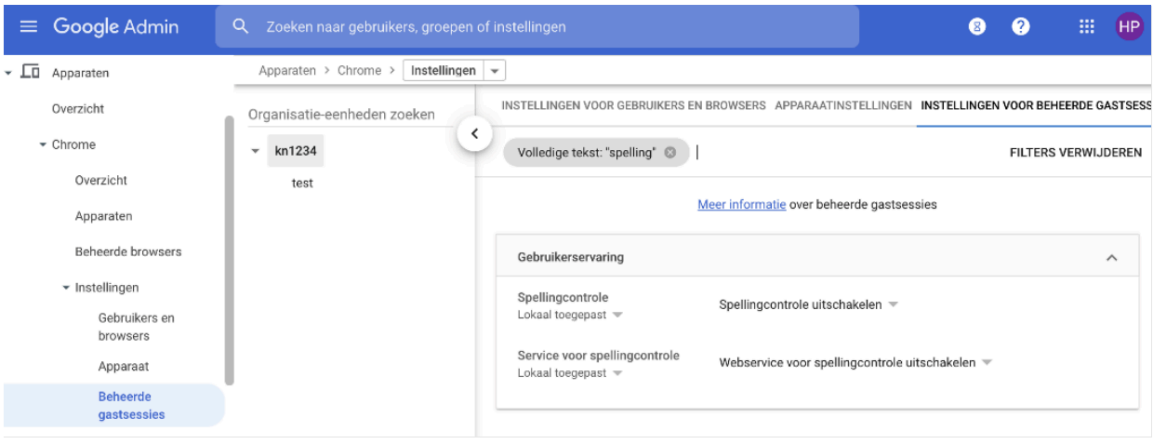
Bei einer verwalteten Gastsitzung startet der Benutzer das Chromebook-Betriebssystem als Gast und nicht als Benutzer. Die Einstellungen des Geräts, u. a. für die Netzwerk- und Druckerverwaltung, werden jedoch zentral vom ICT-Administrator verwaltet. Die Speicherung von Dateien auf dem Gerät ist temporär. Wenn Sie zum Beispiel ein Bild herunterladen, wird es automatisch gelöscht, wenn das Chromebook geschlossen wird. Außerdem wird während einer verwalteten Gastsitzung auch der Chrome-Browser immer im Gastmodus geöffnet. Alle browserbezogenen Daten (Formulare, Browserverlauf, Cookies und Anmeldesitzungen auf Websites und Webanwendungen) sind temporär und werden beim Schließen des Geräts gelöscht

Wenn Sie ein Chromebook verwalten, können Sie wählen, ob Sie ein Chromebook ohne Benutzerkonten verwenden möchten. Dies erreichen Sie, indem Sie das Chromebook automatisch in einer verwalteten Gastsitzung starten. Führen Sie dies in der Workspace Admin konsole unter Geräte > Chrome > Einstellungen > Einstellungen für verwaltete Gastsitzungen > Verwaltete Gastsitzung automatisch starten aus.

Dieses Handbuch enthält Einstellungen, die für Benutzer und Browser gelten. Diese können über **Geräte > Chrome > Einstellungen > Benutzer- und Browsereinstellungen** eingestellt werden. Wenn Sie Chromebooks in verwalteten Gastsitzungen innerhalb Ihrer Organisation verwenden, müssen Sie alle diese Einstellungen auch für die Gastsitzungen unter **Geräte > Chrome > Einstellungen > Einstellungen für verwaltete Gastsitzunge**n vornehmen.

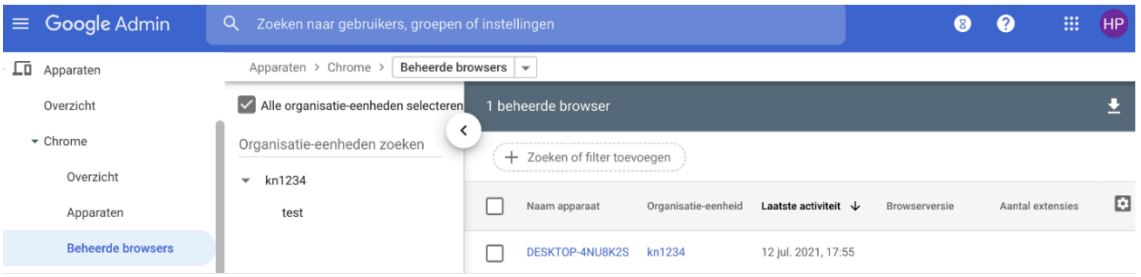
Als Beispiel finden Sie unten die Einstellungen für die Rechtschreibprüfung. Alle für Benutzer und Browser beschriebenen Einstellungen müssen daher auch für die verwaltete Gastsitzung vorgenommen werden.

Beispiel: Deaktivieren Sie den Webdienst für die Rechtschreibprüfung für verwaltete Gastsitzungen unter: **Geräte > Chrome > Einstellungen > Einstellungen für verwaltete Gastsitzungen**.




## 4.4 Chrome-Browser unter Verwaltung stellen

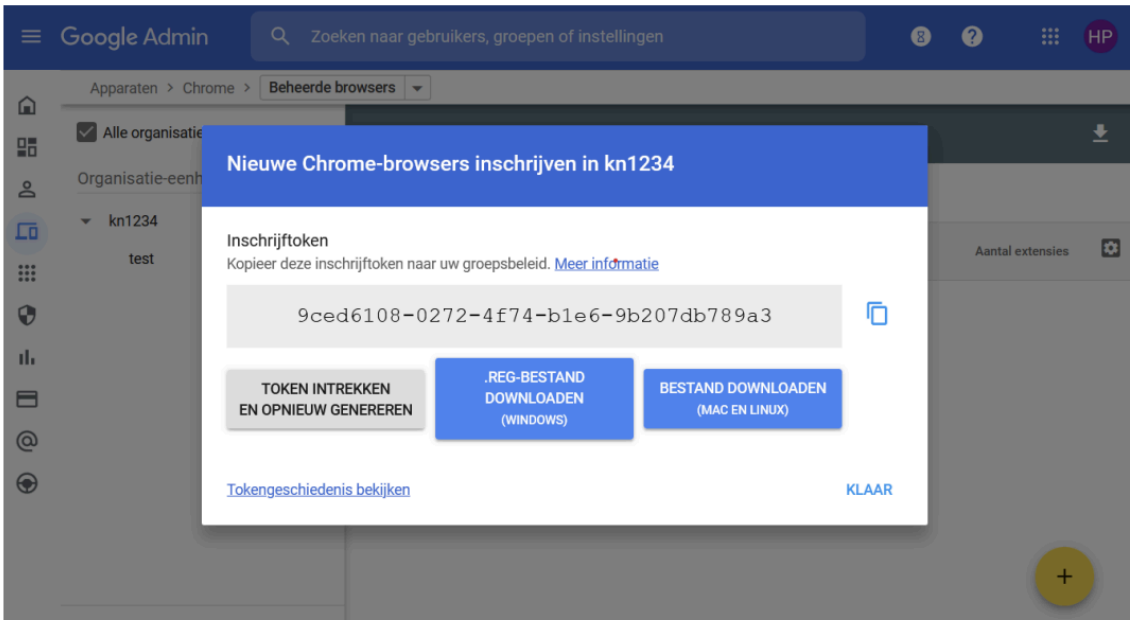
Sie können die Einstellungen von Chrome-Browsern nur dann zentral verwalten, wenn diese verwaltet werden. Dies kann in der Verwaltungskonsole überprüft werden unter **Geräte > Chrome > Verwaltete Browser**




Wenn Sie ein anderes Betriebssystem wie Windows oder Mac verwenden, dann führen Sie die folgenden Schritte aus:

1. Erzeugen Sie ein Token für die Verwaltung über die Admin Konsole.
2. Richten Sie eine Verwaltungsrichtlinie mit dem Administrator-Token auf Ihrem Betriebssystem ein.

Sie erstellen das Token unter **Geräte > Chrome > Verwaltete Browser**. Klicken Sie unten rechts auf dem Bildschirm auf das gelbe Pluszeichen ("+").




Sie installieren den Token gemäß der Gruppenrichtlinie Ihres Betriebssystems über die Richtlinie „CloudManagementEnrollmentToken“. Nachfolgend können Sie mehr über Gruppenrichtlinien lesen.

### 4.5 Einstellungen am Betriebssystem über Gruppenrichtlinien

Einige der zu ergreifenden Maßnahmen können über eine sogenannte „Gruppenrichtlinie“ direkt auf dem Betriebssystem umgesetzt werden. Die Betriebssystemeinstellungen haben Vorrang vor den über die Admin-Konsole festgelegten Einstellungen. Die Übersichtstabelle der Maßnahmen zeigt, welche Richtlinien Sie wie per Gruppenrichtlinie festlegen können.

Als Administrator verwenden Sie oder Ihr Anbieter ein sogenanntes Gruppenrichtlinien-Verwaltungstool, um Gruppenrichtlinien zu verwalten. Die allgemeine Verwaltung der Geräte in Ihrem Unternehmen geht über den Rahmen dieses Handbuchs hinaus. Wenden Sie sich dazu bitte an Ihren Lieferanten.

Weitere Informationen zu den Einstellungen über das Betriebssystem finden Sie auf der Seite Liste vonChrome Enterprise-Richtlinie.

## 5 Einstellungen in der Admin-Konsole

Maßnahmen, die den Nutzer und zugehörige Nutzerkonten betreffen, können häufig zentral über die Google Workspace-Umgebung in der Admin-Konsole eingestellt werden. Sie erreichen diese Verwaltungsumgebung über admin.google.com.

### 5.1 Richten Sie Google Workspace als K-12 ein

Die Schulpflicht in den Vereinigten Staaten dauert dreizehn Jahre. Es beginnt mit einem Jahr Kindergarten, gefolgt von 12 Jahren Unterricht im Klassenzimmer, von der ersten bis zur zwölften Klasse. Deshalb wird dieses System K-through-12 oder K-12 genannt. K-12 entspricht in etwa der Primar- und Sekundarschulbildung in den Niederlanden.

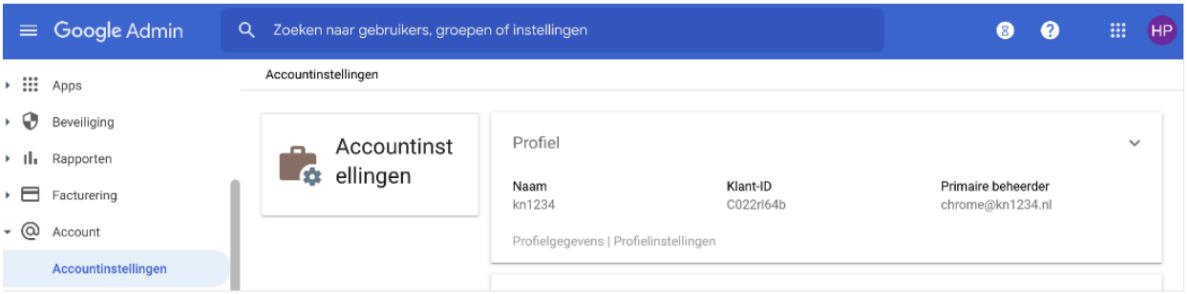
Um die Privatsphäre von Kindern an diesen „K-12-Schulen“ zu schützen, verfügt Google Workspace for Education über eine spezielle K-12-Einstellung. Mit dieser Einstellung sind alle Personalisierungseinstellungen deaktiviert. Die Nutzung von Google Workspace als K-12-Schule bietet das höchste Maß an Schutz für personenbezogene Daten. Auch Bildungseinrichtungen in anderen Bereichen als der Primar- und Sekundarstufe haben die Möglichkeit, sich für die Einrichtung dieser K-12-Einstellungen zu entscheiden. Google prüft nicht, ob es sich bei der Bildungseinrichtung um eine K-12-Einrichtung handelt oder ob Google diese Einstellungen freiwillig auf seine eigene Organisation anwendet. Wenn Sie sich für diese Einstellung entscheiden, entscheiden Sie sich für ***Datenschutz standardmäßig*****:** eine der Anforderungen der DSGVO.

Wählt man die Option K12, werden verschiedene Einstellungen automatisch umgesetzt, wodurch die Privatsphäre der Nutzer standardmäßig (besser) geschützt wird. Die Standardmaße sind:

- Personalisierte Anzeigen sind deaktiviert
- Der Zugriff auf zusätzliche Dienste ist deaktiviert
- Der Zugriff auf den Google-Marketplace ist deaktiviert

Wenn der gesamten Organisation das Attribut K12 erhält, werden viele Funktionen, die Sie möglicherweise für Lehrer zulassen möchten, deaktiviert. Es ist daher nicht notwendig, die gesamte Organisation auf K12 zu setzen. Dies kann pro Organisationseinheit erfolgen. Beispielsweise 1 Organisationseinheit für Studierende und 1 für Lehrkräfte. Weitere Informationen hierzu finden Sie unter diese Seite.

Wählen Sie in der Admin-Konsole von Google Workspace unter: **Kontoeinstellungen > Profil > Organisationstyp** den Organisationstyp „**Primäre/sekundäre Bildung**“ aus.




## 5.2 Benutzernamen in E-Mail-Adressen

Es wird empfohlen, in der E-Mail-Adresse keine Namen von Mitarbeitern, Schülern oder Studenten zu verwenden. Machen Sie E-Mail-Adressen anonym oder zumindest weniger nachvollziehbar. Beispielsweise indem Sie in der E-Mail-Adresse anstelle des Namens die eindeutige Matrikel- oder Mitarbeiternummer verwenden. Also Schüler123@school.nl statt jan.jansen@school.nl. Diese Maßnahme gewährleistet einen besseren Schutz der Privatsphäre des Schülers, da aus der E-Mail-Adresse keine Rückschlüsse auf die Person gezogen werden können.

Warum diese Maßnahme? Ein Beispiel: Sie haben alle eine E-Mail für ein Meeting mit einer riesigen Liste von Personen erhalten, die im CC sichtbar sind. Es handelt sich tatsächlich um eine Datenpanne. Durch die Verwendung anonymer E-Mail-Adressen, zumindest für Kinder, verhindern Sie derartige Lecks.

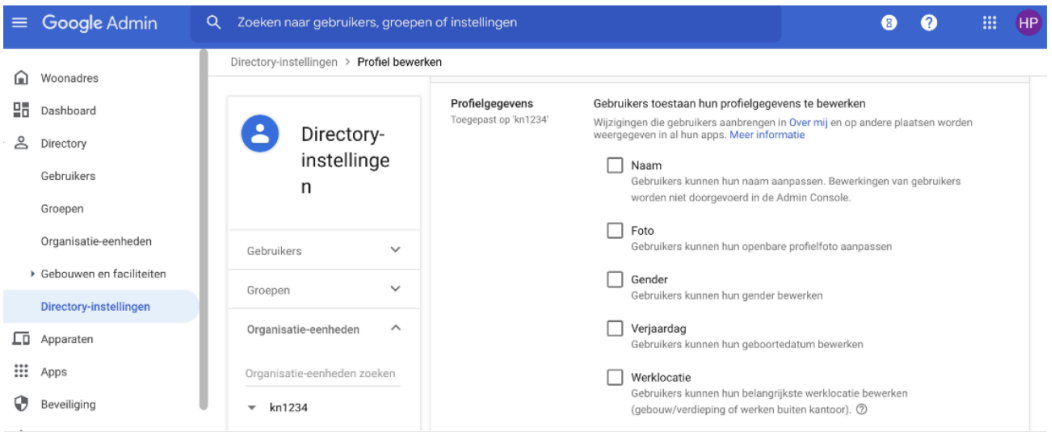
Da die E-Mail-Adresse und die Matrikelnummer im Verzeichnis mit anderen Daten über den Studenten verknüpft sind, bleibt der Student innerhalb der Organisation und auch für Google identifizierbar. Vor- und Nachname sind also im Verzeichnis enthalten, aber nicht in der E-Mail-Adresse. Wenn Sie also eine E-Mail von leerling123@school.nl erhalten, wird in Google Mail der Name des Schülers mit dieser E-Mail-Adresse angezeigt.  Wenn die E-Mail-Adresse jedoch bekannt wird (außerhalb der Google-Umgebung), wird der Name des Schülers nicht angezeigt.

Bitte beachten Sie: Wenn die E-Mail-Adresse als eindeutige Kennung für das Single Sign-On mit anderen Systemen verwendet wird, ist die Umstellung auf eine anonyme E-Mail-Adresse schwieriger. Sie können sich dann dafür entscheiden, die bestehenden Konten unverändert zu lassen und die neuen Konten zu anonymisieren. Diesen Ansatz beschreiben Sie dann in der lokalen DSFA. Das Verwaltungskonto kann auch einen fiktiven Namen haben. Dies ist im beschrieben [Datenschutz-Implementierungsleitfaden für Workspace for Education.]

## 5.3 Benutzerprofile

Administratoren können festlegen, dass Nutzer ihre Profile nicht bearbeiten können. Dadurch wird verhindert, dass Mitarbeiter, Schüler oder Studenten weitere persönliche Daten hinzufügen und ihre Profile mit sensiblen Daten ergänzen.

Einstellen unter: **Verzeichniseinstellungen > Profil** bearbeiten



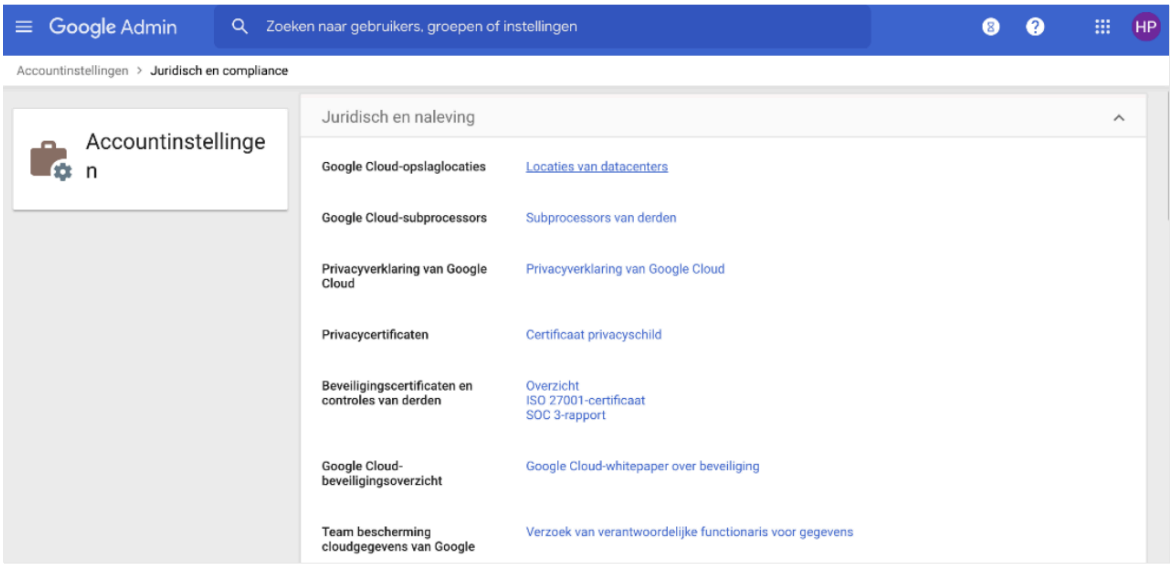
## 5.4 Geografischer Standort der Datenspeicherung

Als Administrator können Sie mithilfe einer Data Region Richtlinie bestimmte Daten an einem bestimmten geografischen Standort speichern. Als geografische Standortoptionen stehen die USA und Europa zur Verfügung.

Die Datenspeicherung in Europa bietet Ihnen den höchsten Schutz personenbezogener Daten. Um Europa als Datenspeicher einzurichten, benötigen Sie die **Education-Standard- oder Plus-Version von Workspace** for Education.

Die Möglichkeit, Daten innerhalb Europas zu speichern, ist nur in den kostenpflichtigen Versionen von Google Workspace for Education enthalten. Die Speicherung von Daten innerhalb Europas ist eine der Maßnahmen, die ergriffen werden können, um das Datenschutzrisiko beim Datenaustausch mit den Vereinigten Staaten zu begrenzen. Im Update DPIA-Bericht vom 2. August 2021 [https://sivon.nl/wp-content/uploads/2022/07/Update-DPIA-report-Google-Workspace-for-Education-2-augustus 2021.pdf] heißt es: „ Datenspeicherung in der EU, sofern möglich. Wählen Sie daher die Speicherung innerhalb Europas, sofern dies (technisch) möglich ist. SIVON arbeitet noch an einer Datentransfer-Folgenabschätzung (DTIA). Diese wurde im Juli 2024 fertiggestellt und ist auf der SIVON-Website zu finden.

Richten Sie es unter **> Admin-Konsole > Kontoeinstellungen > Recht und Compliance** ein.




## 5.5 Zusätzliche Google-Dienste (Zusatzdienste)

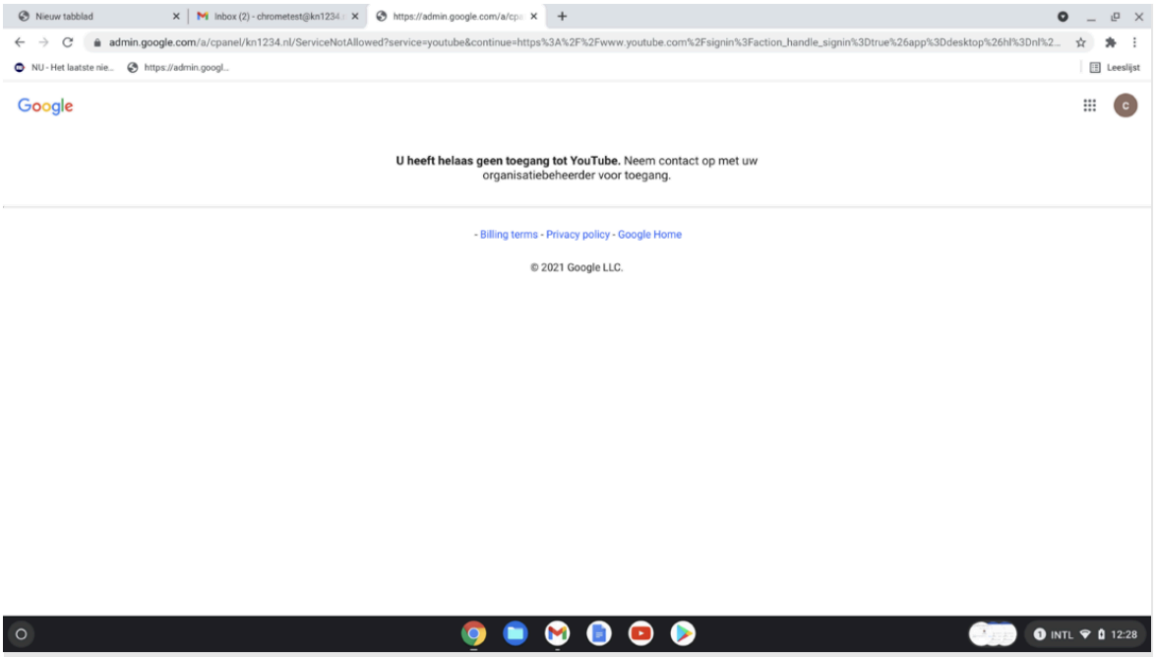
Zusätzliche Google-Dienste sind nicht durch die Google Workspace-Vereinbarung abgedeckt, die SURF und SIVON mit Google abgeschlossen haben. Diese zusätzlichen Dienste müssen daher deaktiviert werden.

Durch die Nutzung dieser Zusatzdienste würden Bildungseinrichtungen Google Zugriff auf Informationen über ihre Mitarbeiter, Schüler oder Studenten gewähren, ohne dass die Bildungseinrichtungen die volle Kontrolle über ihre Daten behalten. Das würde gegen die DSGVO verstoßen. Es bedeutet, dass der Zugriff auf zusätzliche Dienste (standardmäßig) deaktiviert werden sollte.

- Wenn der Zugriff auf zusätzliche Dienste gesperrt ist, können Mitarbeiter, Schüler oder Studenten weiterhin die Google-Suche trotzdem nutzen, da die automatische Abmeldung im SafeSearch-Modus aktiviert ist. Dies bedeutet, dass sie von Google nicht nachverfolgt werden, da sie "unsichtbar" abgemeldet sind, so dass Google den Nutzer der Suche nicht kennt.  Auch die Nutzung einer datenschutzfreundlichen Suchmaschine wie Duck Duck-Go ist möglich.
- Die Nutzung von YouTube durch Mitarbeiter, Schüler oder Studierende ist nicht möglich, solange diese in ihrem Workspace for Education-Konto angemeldet sind. Lehrer können YouTube-Videos nur verwenden, indem sie sie im erweiterten Datenschutzmodus einbetten, z.B. indem sie den (Link zum) Video in Classroom oder Slides einfügen. Das bedeutet, dass Videos weiterhin angesehen werden können.
- Schüler der weiterführenden Berufs- und Hochschulbildung, die sich für die Nutzung von Scholar, YouTube oder anderen Zusatzdiensten entscheiden, müssen sich separat bei Google für ein Verbraucherkonto registrieren. Sie müssen sich von ihrem Workspace for Education-Konto bei der Bildungseinrichtung abmelden. Google und nicht die Universität ist dann dafür verantwortlich, eine gültige Einwilligung dieser Studenten (ab 16 Jahren) für die Datenverarbeitung in solchen privaten Google-Konten einzuholen.

**YouTube**

Da zusätzliche Google-Dienste nicht von der Google Workspace for Education-Vereinbarung abgedeckt sind, müssen diese Dienste ausgeschaltet  werden. YouTube ist einer der zusätzlichen Dienste. Die Nutzung stellt ein hohes Risiko für Mitarbeiter, Schüler oder Studenten dar, da die Schule keine Kontrolle über deren persönliche Daten hat, die Google sammelt oder verwendet. Durch das Deaktivieren der zusätzlichen Dienste können sie sich nicht mehr mit ihrem Google Workspace-Konto bei YouTube anmelden. Das bedeutet, dass sie keine Playlists mehr erstellen oder Videos hochladen können. Sie können jedoch weiterhin Videos im eingebetteten Modus ansehen, wie im technischen Handbuch beschrieben. Wenn Sie den YouTube-Player in den Workspace Core Services (z. B. Websites oder Classroom) einbetten, wird keine Werbung mehr angezeigt. Die YouTube-Cookies des eingebetteten Players entsprechen den neuen Datenschutzbestimmungen.

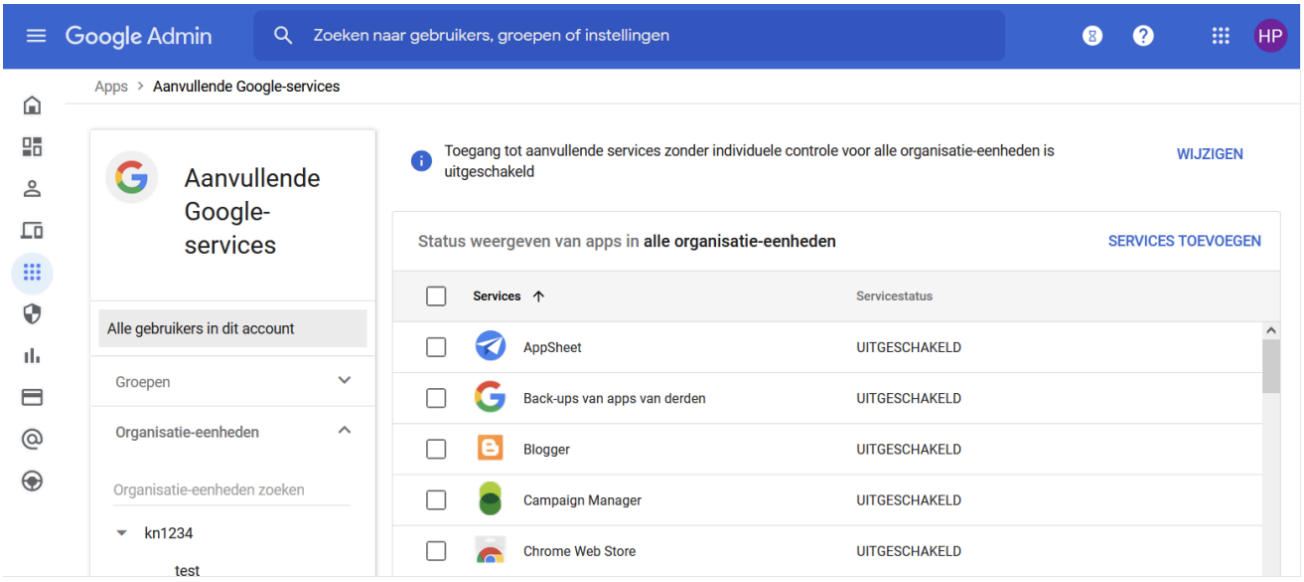


**Youtube-Workaround:**

• Sie können in Google Workspace eine Organisationseinheit erstellen, die von den geltenden Datenschutzeinstellungen abweicht. In dieser Organisationseinheit können Sie einige generische, anonyme Konten erstellen, die Zugriff auf YouTube haben. Wenn diese Konten nicht auf Einzelpersonen zurückgeführt werden können
z.B. youtubebeheer1@school.nl, hat dies kaum oder gar keine Auswirkungen auf den Datenschutz. Sie können dann trotzdem Videos von diesen Konten hochladen.
• Es gibt auch Schulen, die einen Laptop oder Computer verwenden, der nicht oder anonym angemeldet ist. Die Schüler können diesen Laptop oder Computer dann im Unterricht verwenden, um YouTube für Hausaufgaben zu nutzen. Auf diese Weise werden keine persönliche Daten erhoben, so dass kein (hohes) Datenschutzrisiko besteht.
• Bei der Suche nach Videos in duck duck duck go kann das Video eingebettet in den Suchergebnissen angezeigt werden, ohne auf www.youtube.com zu gehen.
• Bitte stellen Sie in jedem Fall sicher, dass kein audiovisuelles Material von erkennbaren Kinder hochgeladen wird. Google ist dafür immer noch der für die Verarbeitung Verantwortliche.

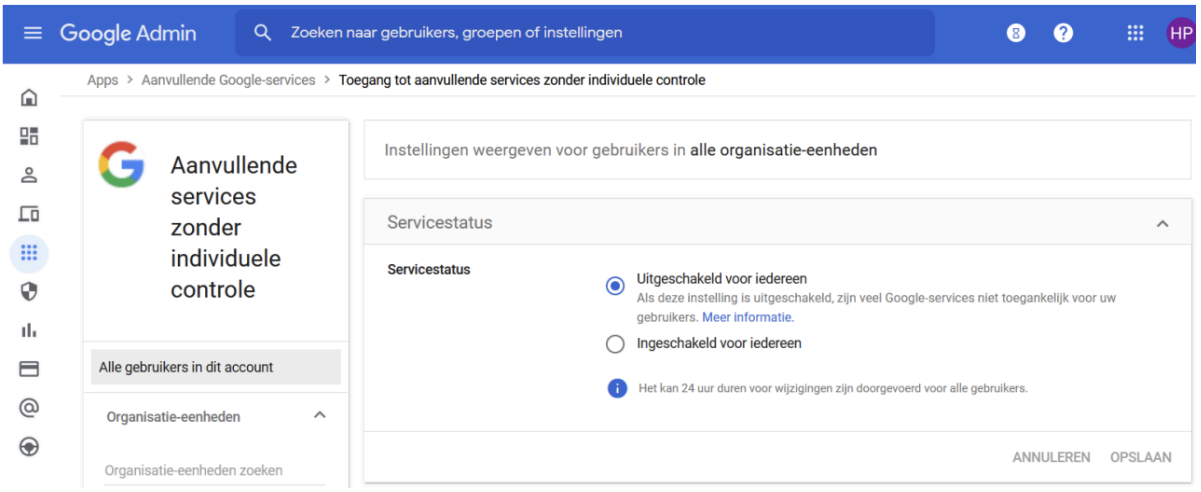
Zusätzliche Dienste können einzeln aktiviert oder deaktiviert werden.

Einstellen unter: **Admin-Konsole > Apps > Zusätzliche Google-Dienste > Für alle deaktivieren**.




Die Einstellung kann auch allgemein für die gesamte Organisation erfolgen.

Einstellung unter: **Apps > Zusätzliche Google-Dienste> Zugriff auf zusätzliche Dienste ohne individuelle Kontrolle > Für alle deaktiviert**.

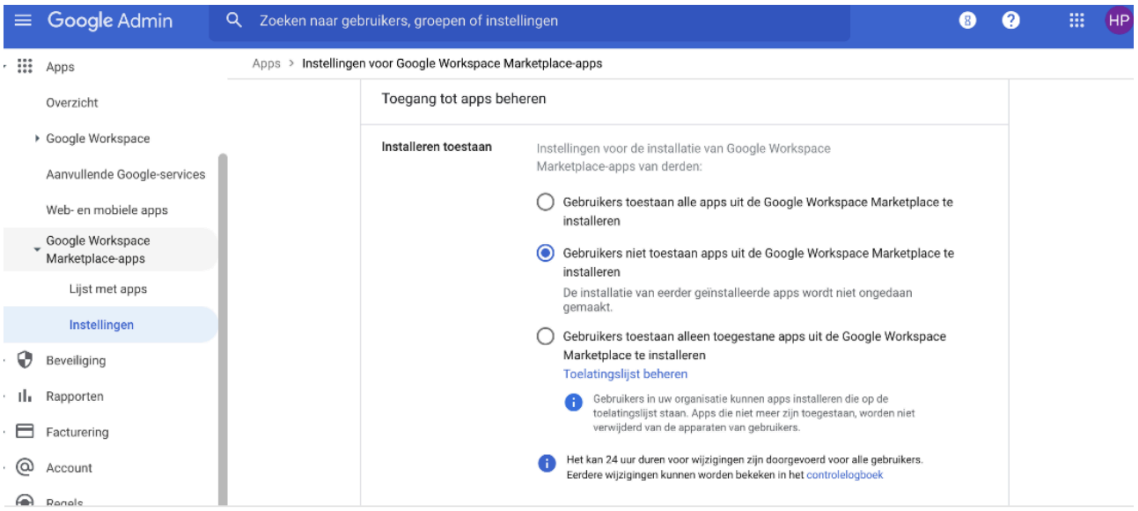



Die Nutzung von YouTube birgt Risiken für den Datenschutz, auch wenn Sie YouTube von einer Microsoft-Umgebung aus nutzen, denn Google zeichnet Ihr Verhalten auf. Nutzen Sie YouTube immer noch? Dann sollten Sie sich darüber im Klaren sein, dass Kinder Werbung sehen werden und Sie keine Kontrolle darüber haben, was Kinder sehen. Um das Tracking von Nutzern zu verhindern, verwenden Sie den eingebetteten Modus wie oben beschrieben oder ein anonymes, gemeinsam genutztes Gerät.

## 5.6 Google Workspace Marketplace-Apps

Die Verwendung aller Arten von (ungeprüften) Marketplace-Apps führt zu Datenschutzrisiken. Wenn Mitarbeiter, Schüler oder Studenten solche Apps über das Workspace for Education-Konto kaufen oder herunterladen, liegt die Verantwortung hierfür bei der Schule. Dies ist nicht wünschenswert, da die Bildungseinrichtung die Kontrolle über die Daten verliert, die an (alle) diese Anbieter gehen. Daher ist diese Option deaktiviert und Mitarbeiter, Schüler und Studenten können nur Marketplace-Apps nutzen, die von der Bildungseinrichtung vorab genehmigt wurden.

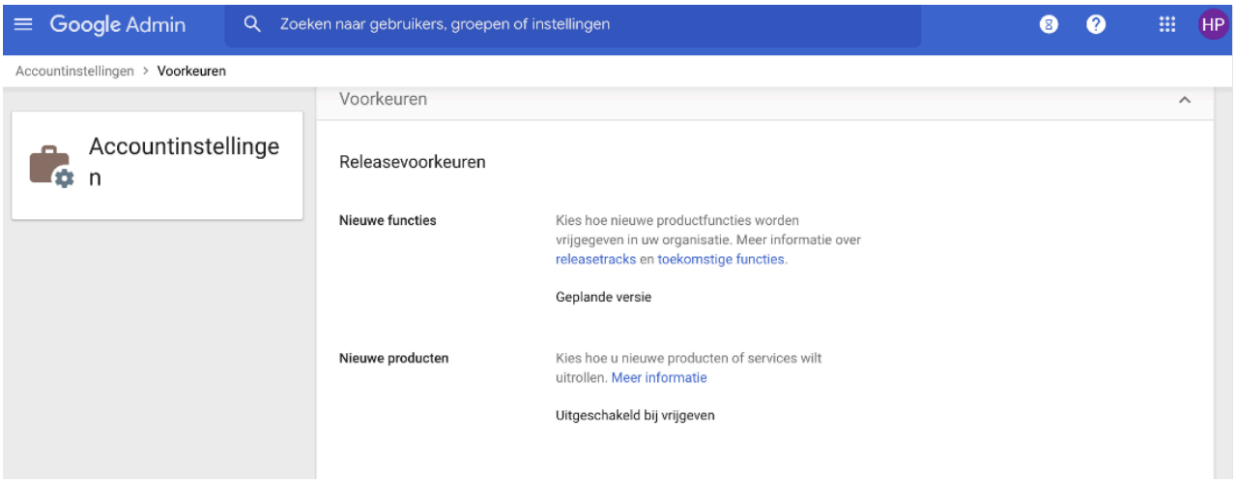
Festlegen unter: **Admin-Konsole > Apps > Google Workspace Marketplace-App-Einstellungen > Benutzern nicht erlauben, Apps aus dem Google Workspace Marketplace zu installieren**.



## 5.7 Neue Google-Produkte

Administratoren können Datenschutzrisiken vermeiden, indem sie Benutzern neue Produkte nicht automatisch zur Verfügung stellen. Neue Dienste können dann zunächst einer Analyse und DSFA unterzogen werden, bevor sie zur Verfügung gestellt werden.

Festlegen unter: **Admin-Konsole > Kontoeinstellungen > Einstellungen > Neue**

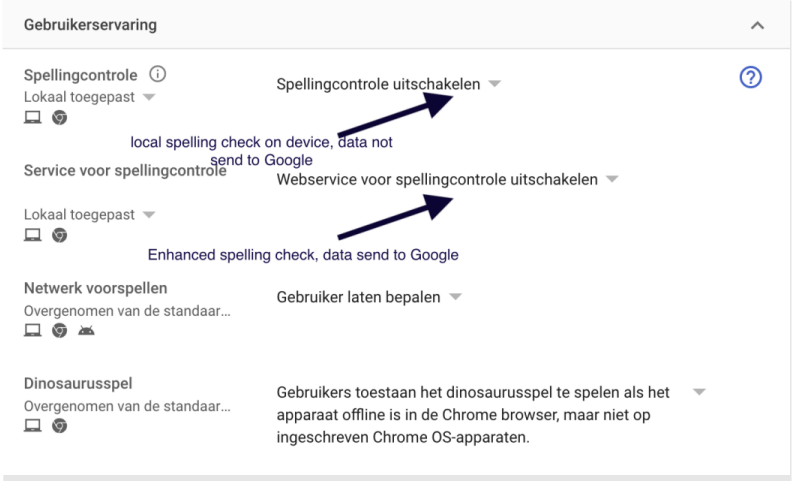



**Produkte > Bei Veröffentlichung deaktivieren**.

## 5.8 Rechtschreibprüfung und Rechtschreibprüfungs-Webdienst

Es gibt zwei Arten von Rechtschreibprüfungen. Die „normale“ lokale Version auf dem Gerät und die „erweiterte“, die mit dem Webdienst funktioniert. Mit der erweiterten Version gehen alle Daten, für die sie eine Rechtschreibprüfung durchführen, an Google. Diese Option muss daher deaktiviert werden. Sie können die lokale Rechtschreibprüfung aktiviert lassen. Der Screenshot zeigt, wie Sie die Rechtschreibprüfung deaktivieren.

Einstellen unter: **Geräte > Chrome > Einstellungen > Benutzer- und Browsereinstellungen > Benutzererfahrung > Rechtschreibprüfung > Webdienste für die Rechtschreibprüfung deaktivieren**.

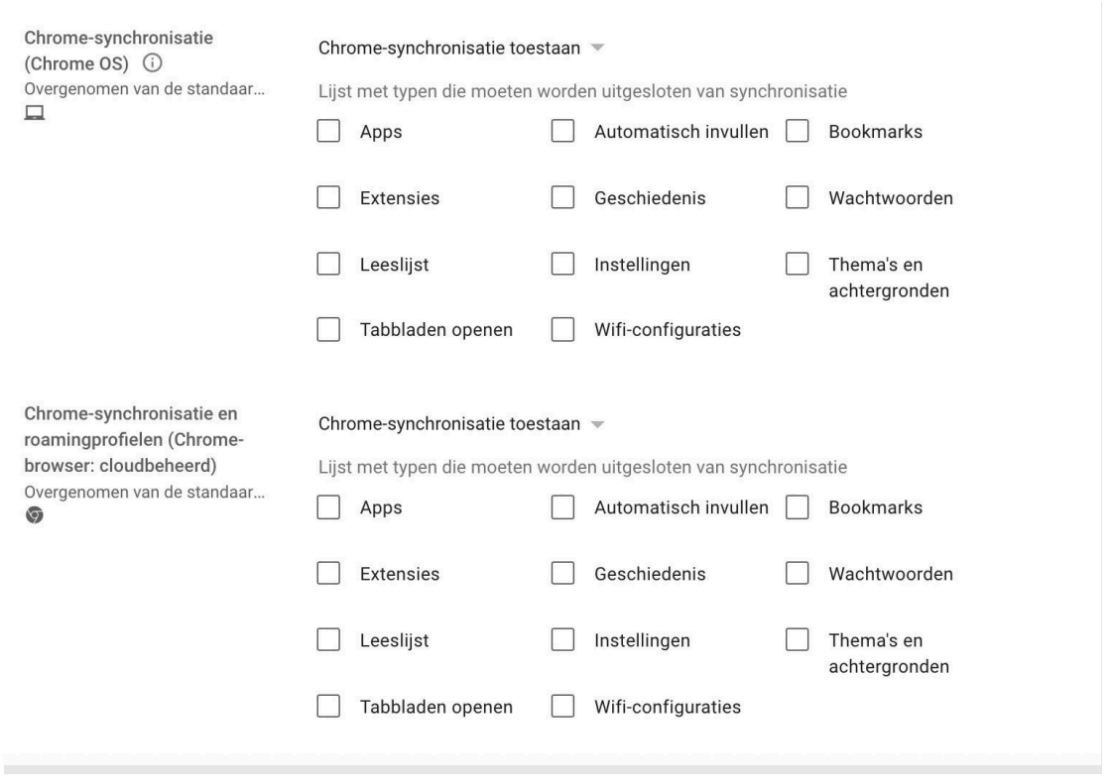


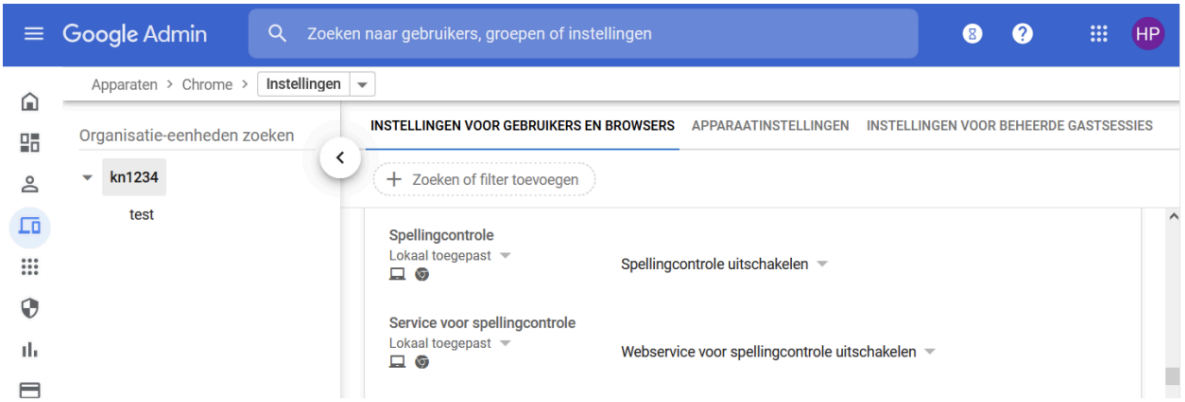
## 5.9 Chrome-Synchronisierung deaktivieren

Der Zweck dieser Einstellung besteht darin, unter anderem die Synchronisierung von Favoriten mit Google und die damit verbundenen Datenschutzrisiken einzuschränken.

Die Synchronisierung der Daten kann durch Einstellung unter: **Geräte > Einstellungen für Benutzer und Browser > Sonstige Einstellungen** verhindert werden

Die DSFA zu Chrome OS und Chrome-Browser empfiehlt Ihnen, die Synchronisierung zu deaktivieren.



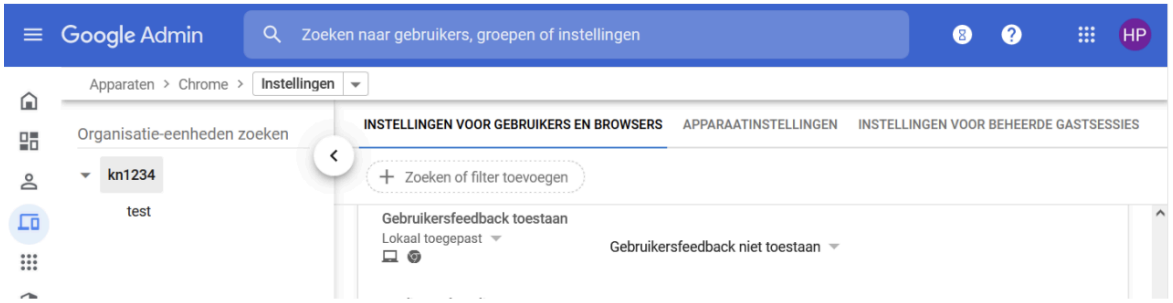

Weitere Informationen finden Sie im Google Chrome Spelling Privacy Whitepaper.
https://www.google.com/intl/en/chrome/privacy/whitepaper.html#spelling

## 5.10 Deaktivieren Sie die automatische Übersetzung von Websites

Was für das Ausschalten der Rechtschreibprüfung gilt, gilt auch für die Übersetzungsfunktion von Google für besuchte Websites. Dies funktioniert natürlich nur, wenn die Daten von Google verarbeitet werden können. Um die Daten nicht weiterzugeben, muss diese Funktionalität deaktiviert werden.

Einstellen unter: **Geräte > Chrome > Einstellungen > Benutzer- und Browsereinstellungen > Benutzererfahrung > Niemals eine Übersetzung vorschlagen**.

Weitere Informationen finden Sie im Google Chrome-Datenschutz-Whitepaper im Abschnitt „Übersetzen“..




## 5.11 Geolokalisierung deaktivieren

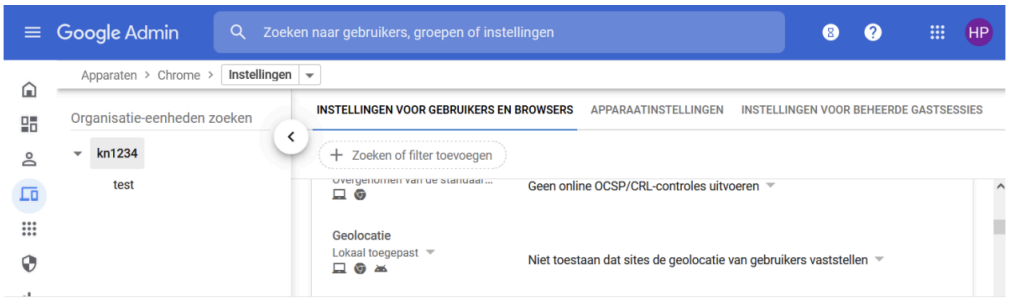
Die Geolokalisierungsfunktion ermöglicht es Websites, den Standort des Benutzers anhand der IP-Adresse zu bestimmen. Durch die Deaktivierung weiß Google (standardmäßig) nicht, wo sich der Nutzer befindet, und begrenzt die Menge der verarbeiteten personenbezogenen Daten. Diese Funktion muss daher ausgeschaltet werden.

Einstellen unter: **Geräte > Chrome > Einstellungen > Benutzer- und Browsereinstellungen > Geolokalisierung > Websites dürfen die Geolokalisierung von Benutzern nicht ermitteln**.

## 5.12 Erlauben Sie kein Benutzerfeedback

Erlauben Sie den Nutzern nicht, ihr Feedback an Google weiterzugeben. Wenn Sie diese Richtlinie nicht festlegen, können die Nutzer ihr Feedback an Google senden. Dies kann die Weitergabe vieler persönlicher oder sogar sensibler Informationen bedeuten, für die Google (und nicht die Bildungseinrichtung) verantwortlich ist.

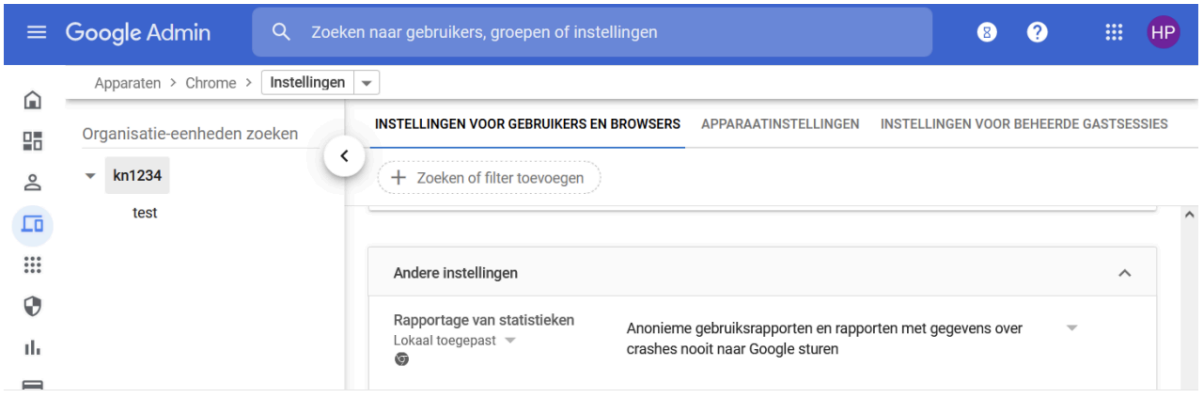
Einstellen unter: **Geräte > Chrome > Benutzer- und Browsereinstellungen > Benutzererfahrung > Benutzerfeedback zulassen > Benutzerfeedback nicht zulassen**.




## 5.13 Statistikberichte: ausschalten

Um Nutzungsstatistiken und Berichte zu erstellen, sammelt Google Daten. Wenn Sie diese Funktion deaktivieren, wird die Menge der von Google verwendeten persönlichen Daten eingeschränkt. Dies verringert die Risiken für die Privatsphäre.

Einstellen unter: **Geräte > Chrome > Einstellungen > Benutzer- und Browsereinstellungen > Weitere Einstellungen > Berichtsstatistiken > Niemals anonyme Nutzerberichte und Berichte mit Daten über Abstürze an Google senden**.



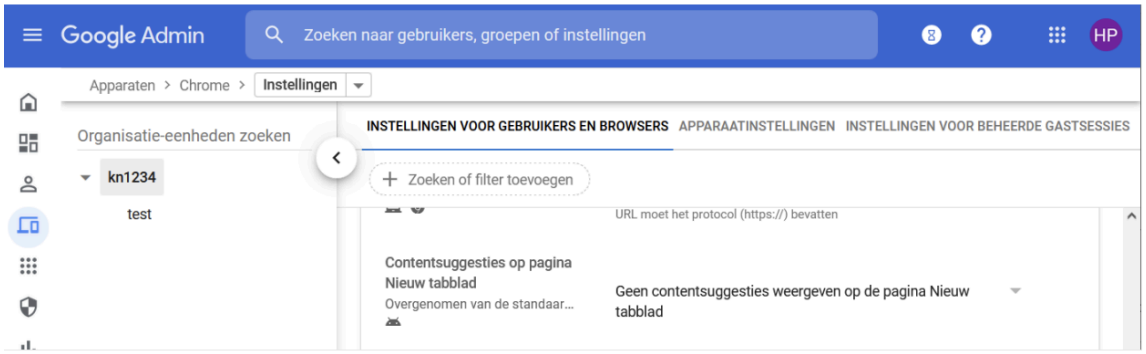

## 5.14 Neue Registerkarte

Neue Registerkarte

Mit einem neuen Tab kann Google dabei helfen, Vorschläge zu machen. Zu diesem Zweck erfasst Google Informationen darüber, welche Websites der Nutzer besucht. Dies ist nicht wünschenswert, da die Menge der verarbeiteten personenbezogenen Daten so gering wie möglich sein sollte. Daher muss diese Einstellung deaktiviert werden.

In der Verwaltungskonsole gibt es unter **Geräte > Chrome > Einstellungen** drei Stellen, an denen die Richtlinie für neue Tabs geändert werden sollte.

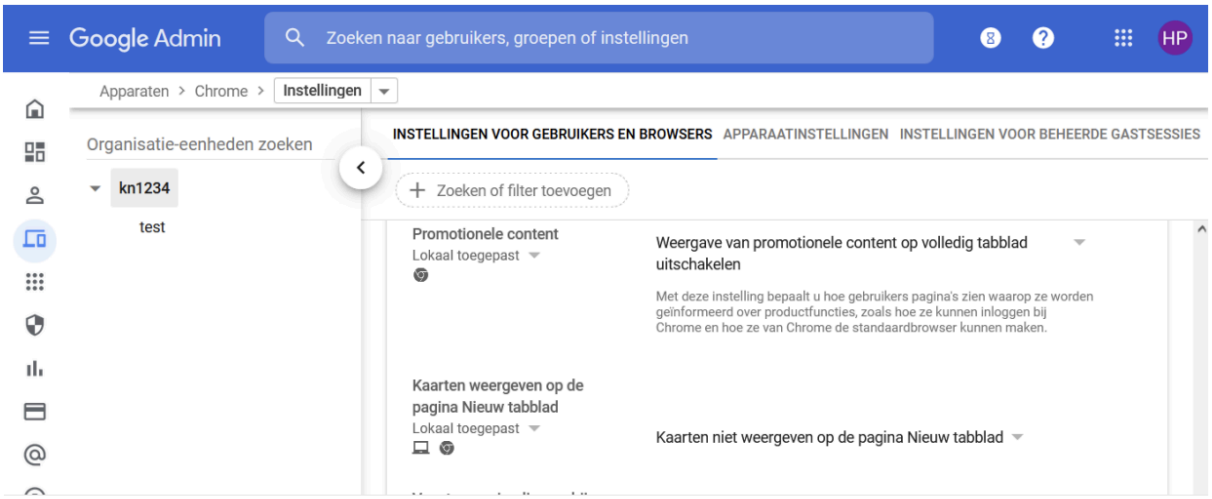
1) **Geräte > Chrome > Benutzer- und Browsereinstellungen > Inhaltsvorschläge nicht auf der Seite „Neuer Tab“ anzeigen**.




2) **Geräte > Chrome > Benutzer- und Browsereinstellungen > Anzeige von Werbeinhalten im vollständigen Tab deaktivieren**.

3) **Geräte > Chrome > Benutzer- und Browsereinstellungen > Karten auf der neuen Registerkarte nicht anzeigen**.

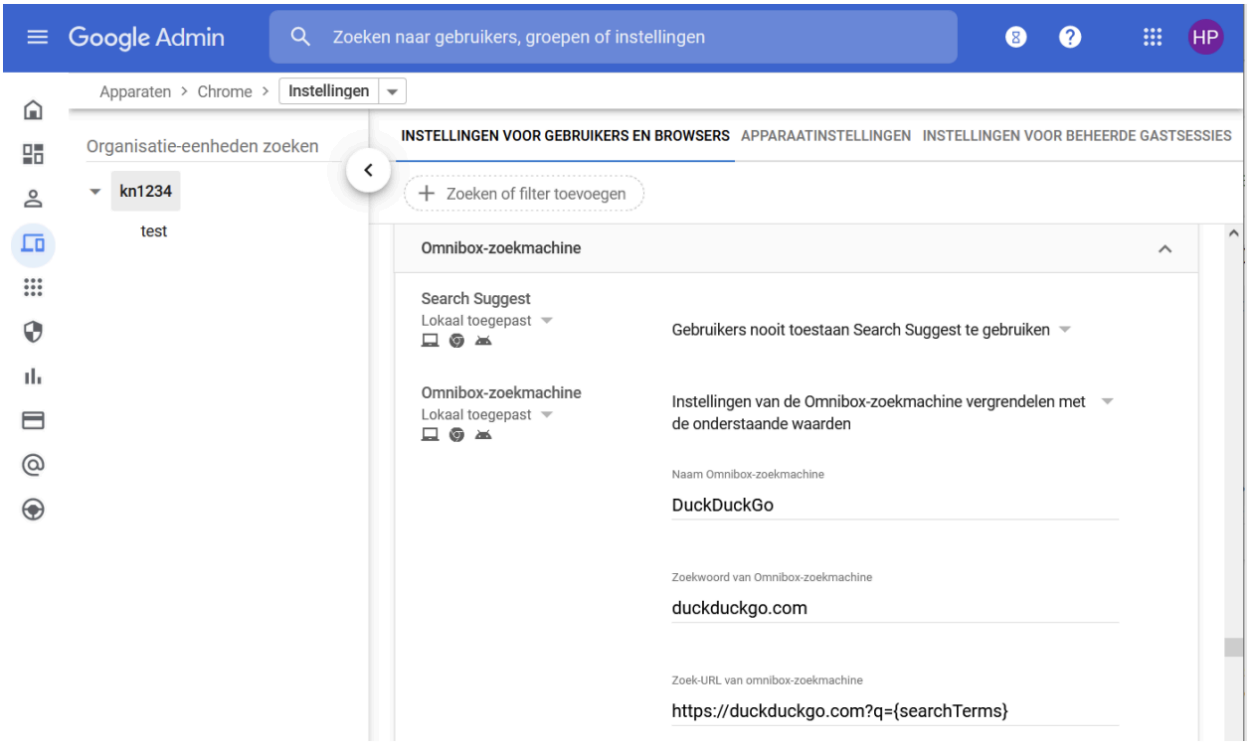
Karten sind „Schaltflächen“ im neuen Fenster häufig besuchter Websites oder beliebten Websites, die von Google ausgewählt werden, wenn noch kein Browserverlauf vorhanden ist.




## 5.15 Vorgeschlagenen Dienst durchsuchen (Omnibox)

Die Funktion *Suchvorschläge herunterladen* wird angemeldeten Benutzern angezeigt, wenn ein neuer Tab geöffnet wird. Diese Vorschläge erfordern, dass Google den Webbrowser-Verlauf speichert. Um die Erfassung und Weitergabe dieser personenbezogenen Daten an Google zu verhindern, muss diese Funktion deaktiviert werden.

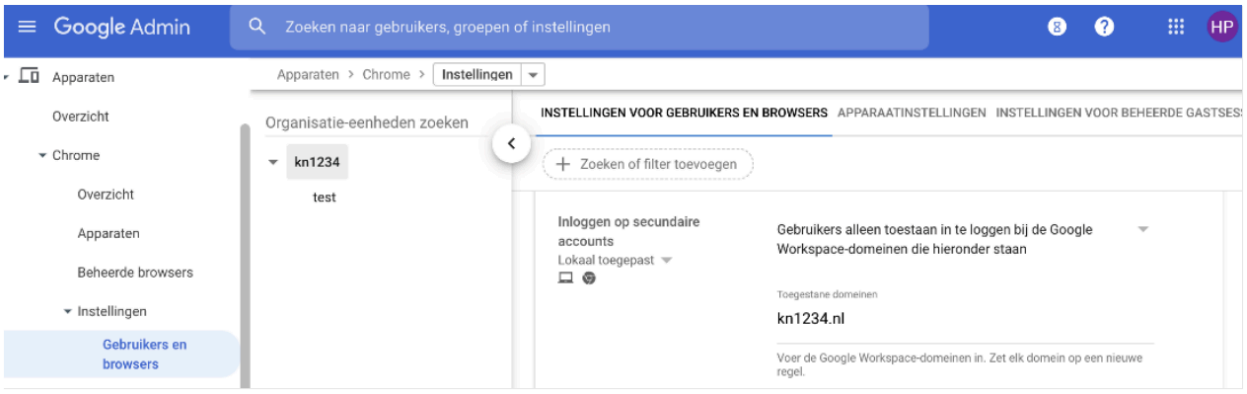
Einstellen unter: **Geräte > Chrome > Einstellungen > Benutzer- und Browsereinstellungen > Omnibox-Suchmaschine > Benutzern niemals erlauben, Suchvorschläge zu verwenden.**




## 5.16 Anmeldung bei sekundären Konten

Um zu verhindern, dass Mitarbeiter, Schüler oder Studierende ihr privates Google-Konto mit dem Schulkonto verknüpfen und dadurch weiteren Datenschutzrisiken ausgesetzt sind, muss das Einloggen in Nebenkonten untersagt werden.

Einstellen unter: **Geräte > Chrome > Benutzer- und Browsereinstellungen > Benutzererfahrung > Bei sekundären Konten anmelden > Benutzern nur erlauben, sich bei den unten aufgeführten Workspace-Domänen anzumelden (nur Schuldomäne hinzufügen)**.




## 5.17 Cookie-Richtlinie

Mitarbeiter, Schüler oder Studenten klicken auf „Cookies zustimmen“, ohne zu wissen, womit sie einverstanden sind. Es wird daher empfohlen, bestimmte Cookies zu blockieren.

Es gibt verschiedene Arten von Cookies:

- **Erstanbieter-Cookies** werden von der Website erstellt, die Sie besuchen. Die Website wird in der Adressleiste angezeigt.

- **Drittanbietern Cookies** werden von anderen Websites erstellt. Diese Websites besitzen einige Inhalte (z. B. Werbung oder Bilder), die Sie auf der von Ihnen

besuchten Webseite sehen (oder nicht sehen, z. B. Facebook-Pixel). Diese Drittanbieter-Cookies können funktionale, analytische oder Tracking-Cookies sein. Mithilfe dieser Cookies kann ein Werbetreibender ein Profil über ihr Surfverhalten erstellen. Das bedeutet, dass der Drittanbieter mehr über sie weiß als der Erstanbieter. Dies ist ein schwerwiegender Eingriff in die Privatsphäre.

• **Funktionelle Cookies** sind notwendig, damit eine Website besser funktioniert. Dabei handelt es sich beispielsweise um Dateien, die den Überblick darüber behalten, was sich in einem Warenkorb befindet.
• **Analytische Cookies** werden unter anderem dazu verwendet, Besucherstatistiken zu verfolgen.
• **Tracking-Cookies** verfolgen den Besucher während des Besuchs einer Website und möglicherweise auch danach. Dies dient unter anderem dem Retargeting. Ein Beispiel hierfür ist eine Werbung, die man überall sieht und der man daher „folgt".

**Cookies von Drittanbietern deaktivieren**

Warum funktionieren einige Dienste nicht mehr, wenn Cookies von Drittanbietern deaktiviert sind? In einer Lernumgebung kommen verschiedene Anwendungen zum Einsatz. Manche Anwendungen benötigen Cookies von Drittanbietern, um ordnungsgemäß zu funktionieren. Ein Beispiel ist Google Drive. Wenn die Cookies von Drittanbietern blockiert sind, können Sie nichts von Google Drive herunterladen. Für Google Drive gelten die Nutzungsbedingungen von Google Workspace for Education. Sie können daher die Cookies von Google Drive akzeptieren. Das Akzeptieren von Cookies von Drittanbietern ist jedoch eine globale Einstellung. Das heißt, wenn Sie die Google Drive-Cookies akzeptieren, akzeptieren Sie gleichzeitig alle Cookies von Drittanbietern. Eine Problemumgehung besteht darin, mit Whitelists zu arbeiten. Sie können eine Whitelist mit Websites erstellen, bei denen Sie wissen, dass Cookies von Drittanbietern keine Datenschutzverletzung verursachen. Der Screenshot zeigt, wie sie Whitelists über die Google Workspace Admin Konsole einrichten.


**Cookies automatisch löschen?**

Sie können lokal im Chrome-Browser einstellen, dass die Cookies automatisch gelöscht werden, wenn sie die Sitzung schließen. Dadurch wird die Wirkung der Tracking-Cookies

begrenzt. Sie tun dies wie folgt:

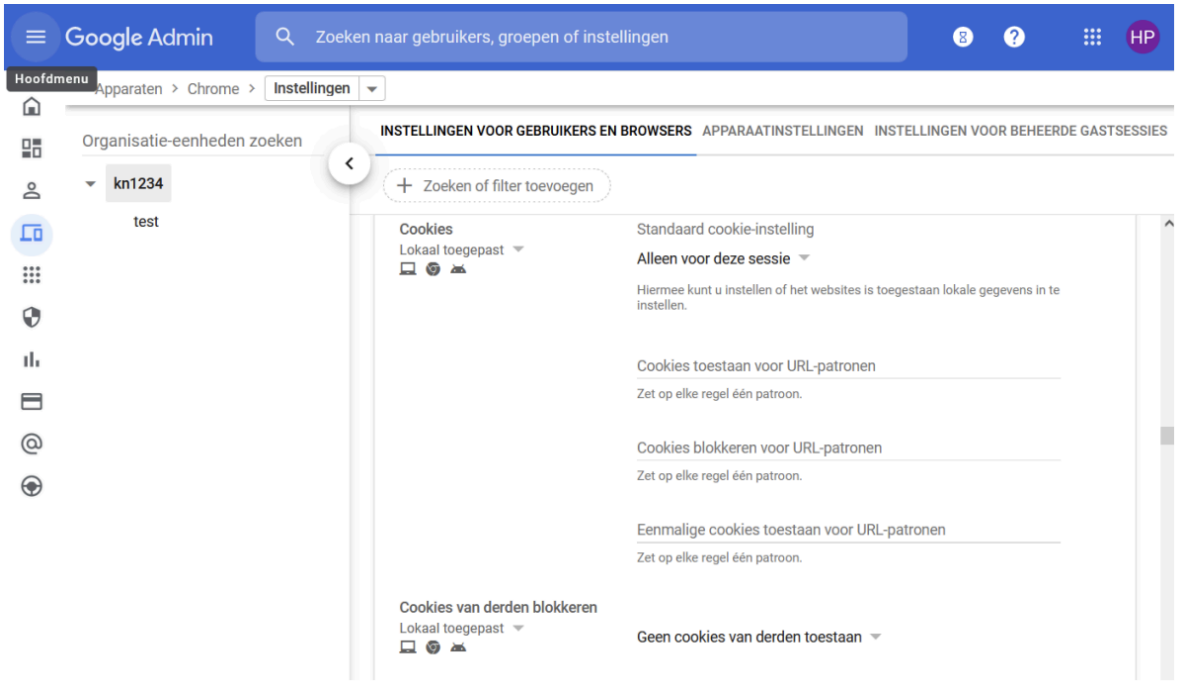
• Klicken Sie oben rechts auf die 3 Punkte > **„Einstellungen“**

• Wählen Sie „**Datenschutz und Sicherheit“ > „Site-Einstellungen“ > „Cookies und andere Site-Daten“**.

• Wählen Sie die Option **„Cookies und Websitedaten löschen, wenn Sie alle Fenster schließen“**

Sie können dies auch zentral in Google Workspace einstellen. Wählen Sie die Cookie-Einstellung **„Nur für diese Sitzung“**. Dies hat den gleichen Effekt.
Diese Maßnahme ermöglicht somit den Einsatz von (Drittanbieter-)Cookies, allerdings werden diese Cookies nicht länger als nötig gespeichert. Wenn das Blockieren von Cookies von Drittanbietern zu großen Problemen bei der Nutzung verschiedener Webanwendungen führt, nutzen einige Schulen diese Option in Kombination mit dem (erzwungenen) Einsatz eines Werbeblockers.

Einstellen unter: **Geräte > Chrome > Benutzer- und Browsereinstellungen > Inhalt > Cookies und Cookies von Drittanbietern**.



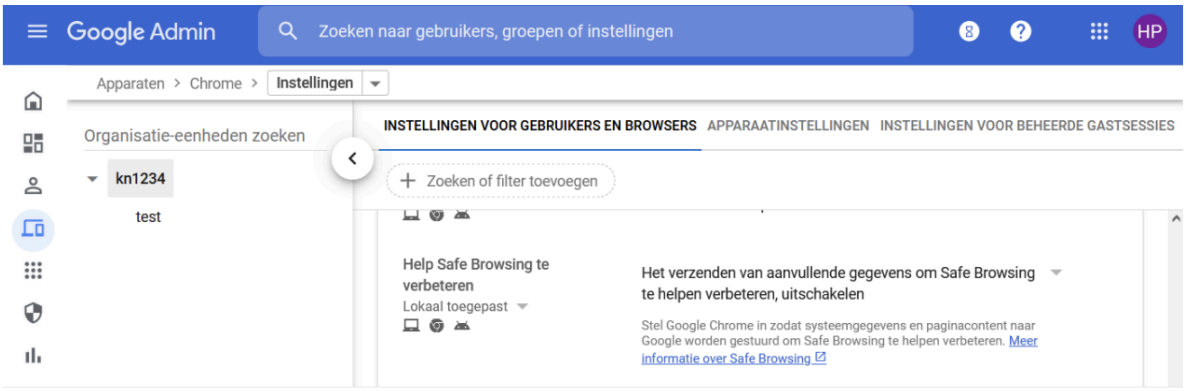

Wenn Kinder über den Browser freien Zugang zum Internet haben, sollten Cookies von Drittanbietern immer blockiert werden. Einfach weil man nie weiß, wer diese Dritten sind und welche Cookies sie setzen. In einer kontrollierten Umgebung haben sie mit allen Anbietern Vereinbarungen zum Datenschutz getroffen, einschließlich des Datenschutzes von Unterauftragsverarbeitern. Angenommen, dieser Anbieter verwendet eingebettete Inhalte von einem Unterauftragsverarbeiter und dieser Unterauftragsverarbeiter setzt Cookies von Drittanbietern, dann fällt dies unter ihre Vereinbarung. Dennoch schadet es nicht, auf unerwünschte Folgen zu achten.

## 5.18 Systemberichte über besuchte Seiten

Für die Funktion „Save Browsing“ sendet der Chrome-Browser regelmäßig

Systeminformationen und den Inhalt der besuchten Seiten an Google. Der Inhalt solcher Seiten kann personenbezogene Daten enthalten, beispielsweise bei der Nutzung von Bildungsressourcen. Es besteht keine Notwendigkeit, diese Informationen zu verfolgen und an Google weiterzugeben. Deaktivieren Sie daher diese Systemberichte.

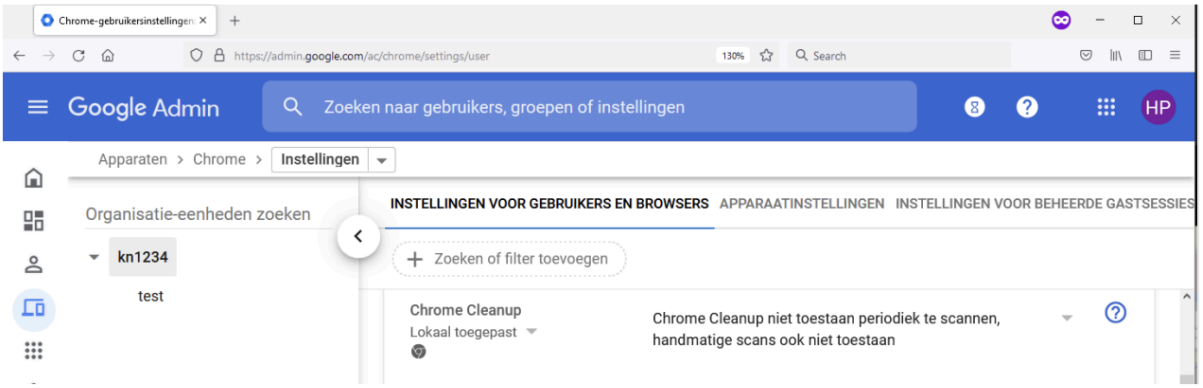
Einstellen unter: **Geräte > Chrome > Benutzer- und Browsereinstellungen > Andere Einstellungen > Zur Verbesserung des sicheren Surfens beitragen > Senden zusätzlicher Daten deaktivieren, um das sichere Surfen zu verbessern**.




### 5.19 Chrome-Cleanup

Chrome Cleanup ist ein Teil des Chrome-Browsers, der regelmäßig den Browser und die Systemumgebung scannt. Um die Datenübertragung zu stoppen, sollten die Ergebnisse der Chrome-Bereinigung niemals an Google weitergegeben werden.

Einstellen unter: **Geräte > Chrome > Benutzer- und Browsereinstellungen > Chrome-Bereinigung > Chrome-Bereinigungsergebnisse werden niemals an Google weitergegeben**.




# 6 Individuelle Einstellungen und Anleitungen

Nur in wenigen Fällen wird ein einzelner Benutzer Maßnahmen ergreifen müssen. Dieses Handbuch geht davon aus, dass die zu ergreifenden Maßnahmen so weit wie möglich zentral verwaltet werden.

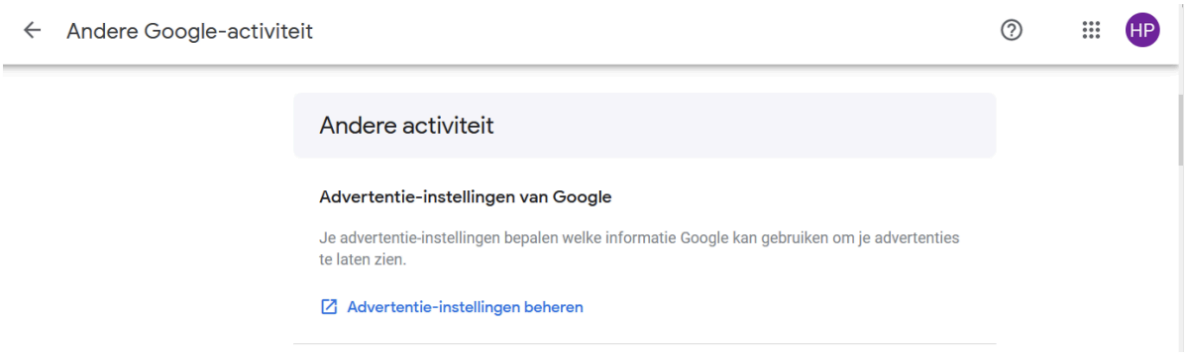
## 6.1 Personalisierung von Werbung

Bitte beachten sie: diese Maßnahme gilt nur, wenn das oben erwähnte "K-12-Profil" **nicht** für die Benutzerkonten eingestellt ist. Bildungseinrichtungen, die sich nicht für K-12 entschieden haben, müssen daher die folgenden Einstellungen manuell selbst vornehmen.

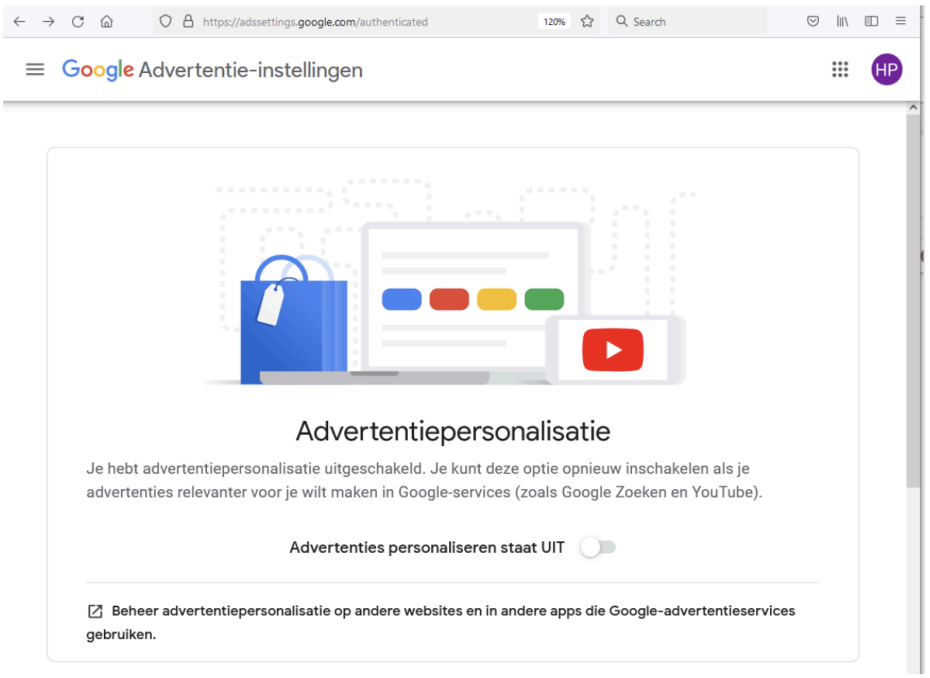
Die einem Nutzer von Google auf Internetseiten angezeigten Werbeanzeigen basieren auf personenbezogenen Daten aus einem Google-Konto, persönlichen Suchanfragen, dem Surfverhalten und einer darauf basierenden Profilerstellung.

Bei der Personalisierung von Werbung werden verschiedene personenbezogene Daten verwendet, die beim Surfen im Internet erfasst werden. Um die Datenübertragung und Entwicklung personenbezogener Daten zu unterbrechen, muss die personalisierte Werbung deaktiviert werden.

Google wird diese Personalisierung von Werbung für neue „Education"-Konten für Workspace for Education deaktivieren. Bestehende Benutzer müssen dies jedoch pro Benutzer auf ihrer eigenen „MyActivity"-Seite über myactivity.google.com ändern.



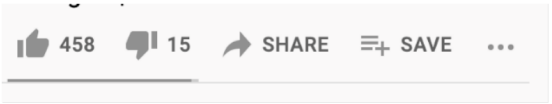

Gehen sie über das Menü zu „**Andere Google-Aktivitäten**" und klicken Sie auf „**Anzeigeneinstellungen verwalten**". Schieben Sie auf dieser Seite die Schaltfläche auf **„Aus**".



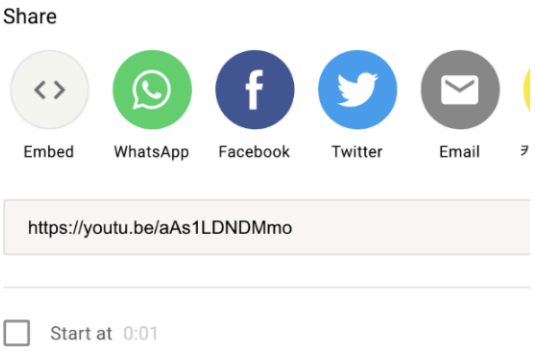
## 6.2 Einbettung von YouTube-Videos

Bei der direkten Nutzung des Zusatzdienstes YouTube erhält Google datenschutzrelevante Trackingdaten. Es wird empfohlen, YouTube-Videos im eingebetteten Modus zu verwenden. Im eingebetteten Modus werden keine Tracking-Cookies verwendet. Wie das geht, wird im Folgenden beschrieben.

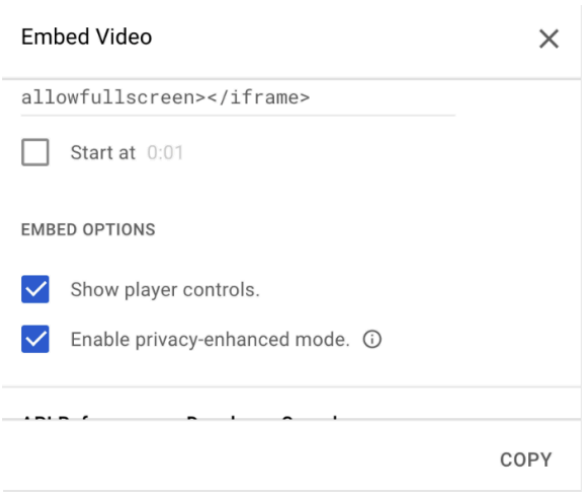
Unter jedem YouTube-Video befindet sich ein Teilen-Button




Klicken Sie darauf, um zum nächsten Bildschirm zu gelangen und wählen Sie **„Einbetten“**.




Anschließend ist es möglich, einen Codeabschnitt mit „Erweiterten Datenschutzmodus aktivieren“ zu kopieren.




Sie können diesen Code dann auf einer Website wie Google Sites veröffentlichen. Von dort aus können Sie nun direkt das YouTube-Video abspielen.

## 6.3 Verwendung des Chrome-Browsers

Am 18. August 2023 wurde eine neue Version des Chrome-Browsers verfügbar, wobei Google als Datenverarbeiter und nicht als Datenverantwortlicher fungiert. Diese Verarbeiter-Version des Chrome-Browsers ist nur auf Chromebooks verfügbar. Für PCs, die

Chrome OS nicht verwenden (Windows, Mac, Linux) empfehlen wir alternative Browser wie Duck Duck Go, Mozilla, Firefox oder Safari.

# 7 Verwenden Sie Google nicht als Suchmaschine

Anstelle der Google-Suche empfehlen wir die Verwendung einer datenschutzfreundlichen Alternative wie DuckDuckGo oder Startpage.

## 7.1 Verwenden Sie einen Werbe- und/oder Tracking-Blocker

Erwägen sie die Verwendung eines Werbe- und/oder Tracking-Blockers. Werbung auf Websites nutzt Tracking, um das Surfverhalten zu verfolgen.

Als Erweiterung im Browser können ein Adblocker (wie uBlock Origin oder Adblock plus) oder Tracking-Blocker (wie Ghostery oder Privacy Badger) installiert werden.

## 7.2 Verwenden Sie keine datenschutzrelevanten Informationen in Datei- und Ordnernamen

Verwenden Sie in Dateinamen oder Ordnern keine Namen von Personen oder andere datenschutzrelevante Informationen. Diese Empfehlung finden sie auch beschrieben in https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_Anleitung.pdf

# 8 Folgenabschätzung für die Datenübertragung

Einer der Punkte, die sich aus der DSFA im Jahr 2021 ergeben, ist die Übermittlung von Daten in die USA. Für diesen Punkt wurde ein gesonderter Prozess gestartet, das sogenannte Data Transfer Impact Assessment (DTIA). Dabei werden die Datenschutzrisiken einer Datenübermittlung in Länder außerhalb des Europäischen Wirtschaftsraums (EWR) untersucht.

Die Untersuchung wurde auf Google Meet durchgeführt.

Für das DTIA wurde das Rosenthal-Modell verwendet. Dieses Modell bewertet 6 Arten der Verarbeitung:
https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx

1. die Inhaltsdaten (Content Data)
2. die Kontodaten (wie E-Mail-Adresse, Name und Passwort)
3. Helpdesk-Daten (Support Daten),
4. Diagnosedaten (über die individuelle Nutzung von Workspace)
5. Sicherheitsdaten, die von Google in Amerika verarbeitet werden, einschließlich Daten über Beschwerden, und
6. Website-Daten (z.B. Cookies).

Das DTIA kommt zu dem Schluss, dass bei der Übermittlung personenbezogener Daten über Meet keine größeren Risiken bestehen.

Es gibt noch eine Reihe wichtiger Maßnahmen, die die Schulen selbst ergreifen müssen, um das Risiko der Weitergabe von Informationen zu verringern.

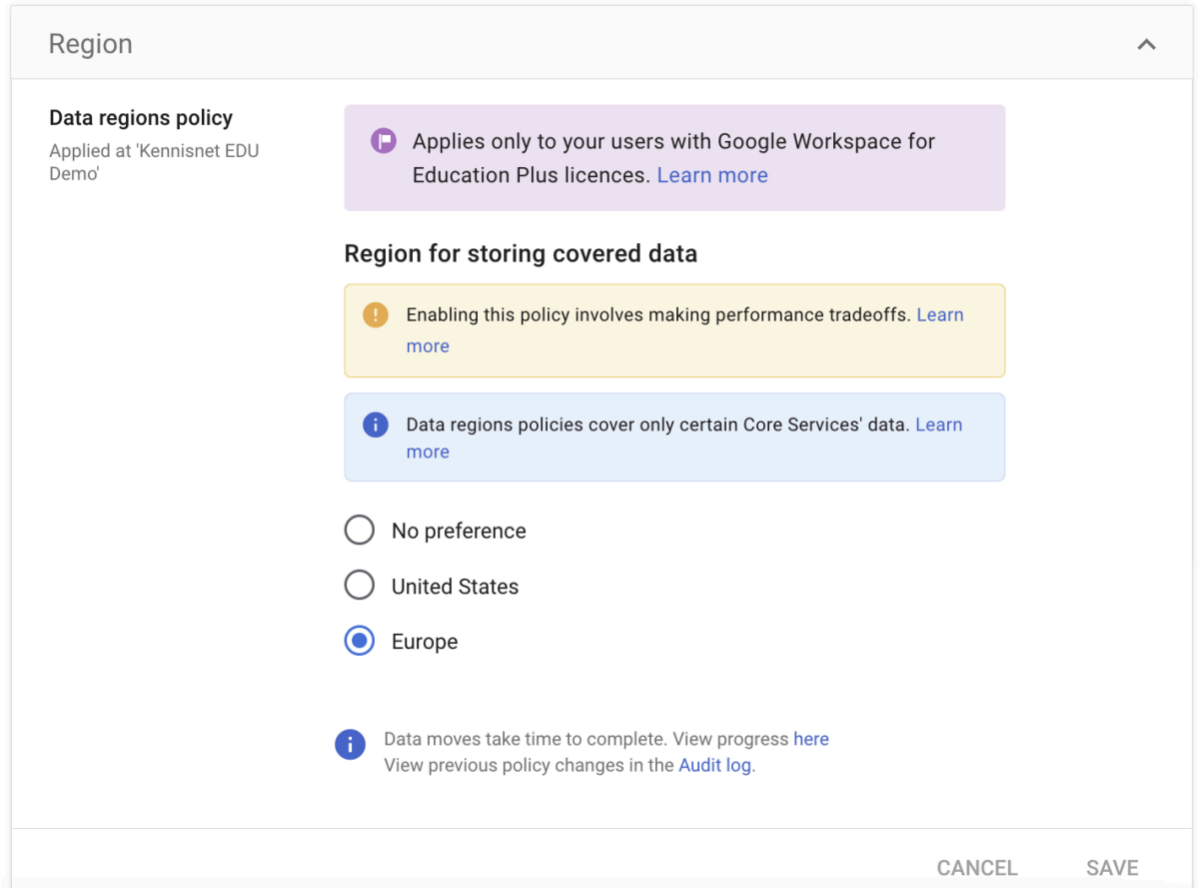
- sich für die Speicherung der Inhaltsdaten in der EU entscheiden.
- Wenn Organisationen erwarten, dass Nutzer **besondere personenbezogene Daten** über Meet austauschen, sollten sie eine clientseitige Verschlüsselung (***Client Side***

***Encryption)*** mit lokaler Schlüsselverwaltung anwenden, um das Risiko eines unbefugten Zugriffs auf diese Daten in Drittländern vollständig auszuschließen.

## 8.1 Data Regions

Melden Sie sich als Administrator unter admin.google.com an und gehen Sie zu **Konto > Kontoeinstellungen > Data Regions -> Europa** auswählen

Diese Funktionalität ist in der Basisversion von Google Workspace for Education nicht verfügbar. Für die Auswahl von Data Regions ist ein Upgrade auf **Google Workspace for Education Standard** oder **Plus** erforderlich.




## 8.2 Clientseitige Verschlüsselung /Client Side Encryption

Schulen, die besondere personenbezogene Daten in Google Workspace verarbeiten möchten, müssen eine clientseitige Verschlüsselung (Client Side Encryption; CSE) mit lokaler Schlüsselverwaltung anwenden, um das Risiko eines unbefugten Zugriffs auf diese Daten in sieben Drittländern vollständig auszuschließen.

Dieses Risiko besteht bei der Risikobewertung von Inhaltsdaten: *Risikobewertung von Inhaltsdaten: Wahrscheinlichkeit, dass eine ausländische Behörde einen Rechtsanspruch auf die Daten hat und diesen gegenüber dem Anbieter durchsetzen möchte*

Das Problem bei der Verschlüsselung in der Cloud besteht darin, dass der Schlüssel Google gehört. Dies ermöglicht es Google, Regierungsbehörden im Rahmen verschiedener Gesetze

Zugriff auf Kundendaten zu gewähren.

Google führt zwei Berichte zur Datenbereitstellung.

1) Weltweit, außer Amerika:
https://transparencyreport.google.com/user-data/overview

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

So geht Google mit Anfragen nach Nutzerdaten im Zusammenhang mit der nationalen Sicherheit in den Vereinigten Staaten um:
https://policies.google.com/terms/information-requests

Bei der clientseitigen Verschlüsselung werden die Daten erneut mit einem Schlüssel verschlüsselt, der sich nicht in der Google Cloud befindet. Google ist dann nicht mehr in der Lage, Kundendaten in einem lesbaren Format an staatliche Stellen weiterzugeben.

CSE Encryption verschlüsselt nur die Inhaltsdaten. Metadaten wie Dateinamen, Labels und die Zugriffskontrollliste bleiben für Google lesbar.

Bei CSE wird der Daten Verschlüsselung Schlüssel (Data Encryption Key; DEK) mit

einem Schlüssel Verschlüsselungs Schlüssel (Key Encryption Key; KEK) verschlüsselt.

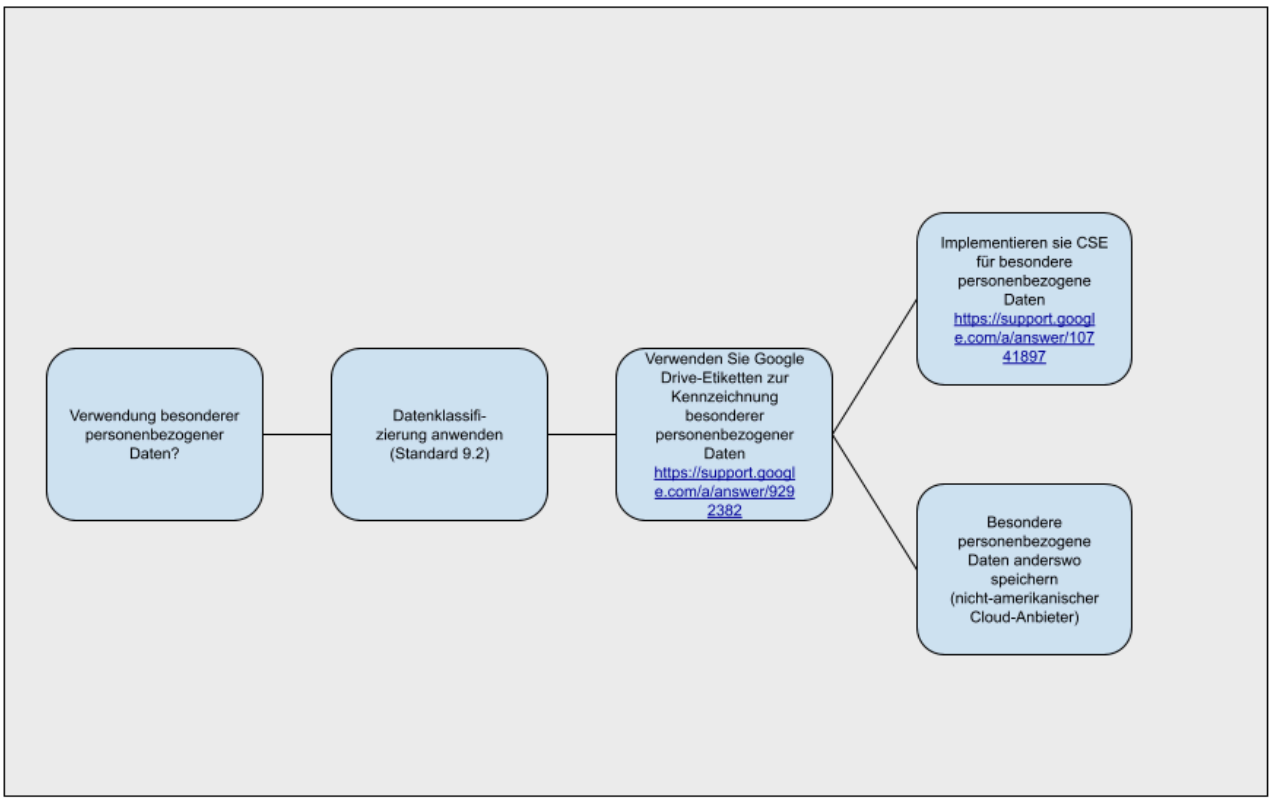
Der KEK wird von einem Schlüsselverwaltungssystem außerhalb der

Google-Umgebung verwaltet.

Quelle:

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

Ansatz:



Wir empfehlen Schulen, die Daten zunächst zu klassifizieren. Die Datenklassifizierung wird in den Standards des IBP-Standardrahmens der Domäne 9 „Datenmanagement“ beschrieben. Die Datenklassifizierung ist erforderlich, um Informationen (normale Daten, spezielle Daten usw.) so zu klassifizieren, dass das richtige Schutzniveau angewendet werden kann. Mit der kostenlosen Lizenz von Google Workspace (Basis Version) können Daten in Google Drive nicht klassifiziert werden. Hierzu ist mindestens die **Google Workspace for Education Standard** Version erforderlich.

https://support.google.com/a/answer/9292382?hl=en&fl=1&sjid=98660791415985355-NA

Die Funktion heißt: **Laufwerksbezeichnungen und -klassifizierung**.

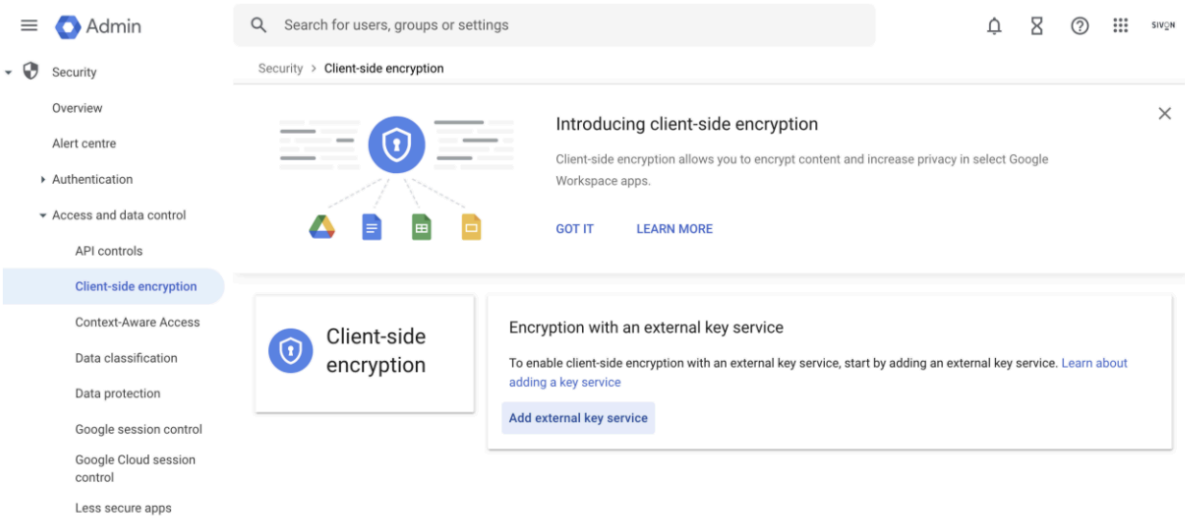
Wenn Schulen spezielle personenbezogene Daten in Google Workspace verarbeiten, muss für diese Daten eine clientseitige Verschlüsselung (CSE) implementiert werden. CSE bietet eine zusätzliche Verschlüsselungsebene, bei der der Schlüssel außerhalb der Google-Umgebung verwaltet wird.

Zusätzlich zu CSE in Google Workspace muss ein Dienst (Schlüsseldienst) verknüpft werden, um die externe Schlüsselverwaltung zu ermöglichen. Bei CSE kann der Schlüssel nicht in der Google Cloud gespeichert werden.

Es gibt drei europäische Anbieter, die Key Management Services anbieten:

- Stormshield
- Flowcrypt
- Thales

Um CSE zu aktivieren, melden Sie sich als Administrator an und gehen Sie zu: **Sicherheit > Zugriffs- und Datenkontrolle > Client-side encryption**




**Einige Funktionen sind bei Verwendung von CSE nicht verfügbar.**

Einschränkungen bei Drive/Doc/Sheets

- Rechtschreib- und Grammatikprüfung im Google Docs-Editor

- Gleichzeitige Bearbeitung mit mehreren Benutzern
- Suchen
- Kommentar hinzufügen

Einschränkungen bei Gmail

- Vertraulicher Modus
- Senden an Gruppen als Empfänger
- Nachrichten durchsuchen
- E-Mail-Signaturen
- Drucken
- E-Mail-Delegierung (gemeinsame Posteingänge)

Einschränkungen im Kalender

- Kalender durchsuchen
- Einschränkungen beim Offline-Verschlüsseln oder Entschlüsseln von Ereignissen mit Meet
- Zeichnen Sie Besprechungen auf
- Live-Streams
- Einwahl für Audio
- Umfragen
- Jamboard
- Anklopfen“ https://workspaceupdates.googleblog.com/2020/08/block-google-meet-participants-from.html
- Verwendung von Hardware für Besprechungsräume
- Einladungen an Teilnehmer außerhalb der Organisation

# Kolophon

## Technischer Leitfaden für Google Workspace for Education

**Datum der Ausstellung**
2. August 2021 (Version 1.0)
20. Juli 2023 (Version 2.0)
31. August 2023 (Version 2.1)
27. Februar 2024 (Version 3.0)

**Autoren**
Version 1.0: Hans-Peter Ligthart (Kennisnet), Job Vos (SIVON), Theresa Song Loong (Kennisnet) Version 2.0: Hans-Peter Ligthart (SIVON)



SIVON und Kennisnet werden vom Ministerium für Bildung, Kultur und Wissenschaft (OCW) finanziert.

Diese Publikation wurde in Zusammenarbeit mit SURF erstellt. **SIVO** 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.



Übersetzt und bearbeitet von datenschutz-schule.info