Maßnahmen für Administratoren von ChromeOS

Problem	**Empfohlene Maßnahmen für Schulen**	**Durch Google getroffene Maßnahmen**
Unvollständige Auskunft bei Auskunftsanfragen (Art. 15 DS-GVO)	Sperren Sie weiterhin zentral den Zugriff auf den Chrome Web Store und den Google Play Store.	Verpflichtung zur Durchführung einer individuellen Bewertung jeder Auskunftsanfrage.
	Verwenden Sie den SIVON-Leitfaden, um die Schüler darüber zu informieren, wie sie den Zugang ihren personenbezogenen Daten sowohl bei der Schule als auch bei Google beantragen können.	Google ist ein Verarbeiter für das domänenweite TakeOut-Tool für Administratoren.
		Google ist ein Verarbeiter für das persönliche TakeOut Tool für Endnutzer/ Betroffene.
		Google hat eine Dokumentation darüber veröffentlicht, welche Diagnose-/ Telemetriedaten die wesentlichen Chrome-Dienste sammeln, und zwar in vielen verschiedenen Hilfeartikeln für jeden Chrome-Dienst, sofern sie überhaupt nutzer- oder gerätebezogene Daten sammeln. Die Hilfeartikel können über Hyperlinks in der Liste mit den wesentlichen und optionalen Chrome-Diensten aufgerufen werden.
		Google hat weitere Informationen zu den Aufbewahrungsfristen für Chrome-Daten in einem Hilfeartikel zu den Aufbewahrungsfristen für Workspace-Daten veröffentlicht.
		Google hat einen **Service Data Downloader** für Administratoren entwickelt.

Maßnahmen für Administratoren von ChromeOS

Problem	**Empfohlene Maßnahmen für Schulen**	**Durch Google getroffene Maßnahmen**
Unzureichende Begründung der Verweigerung des Zugangs zu bestimmten Daten in der Antwort auf ein Auskunftsersuchen	Verwenden Sie als Administrator die verfügbaren Ereignisprotokolle, um Zugang zu personenbezogenen Daten zu erhalten.	Das zentral verwaltete ChromeOS umfasst Funktionen zur Anzeige personenbezogener Daten wie den **Service Data Downloader** und das **Diagnostic Information Tool** (DIT, ein für Workspace entwickelter Viewer für Telemetriedaten). Google hat eine verbesserte Erläuterung zu den personenbezogenen Daten veröffentlicht, die im Rahmen eines Auskunftsersuchens nicht bereitgestellt werden. Google hat eine Dokumentation für Administratoren über die Kategorien personenbezogener Daten veröffentlicht, die für jeden Dienst in den Ereignisprotokollen (event logs) für Administratoren verfügbar ist.
Fehlende Angaben zur Zweckbindung aus dem Takeout-Tool	Blockieren Sie weiterhin „Zusätzliche Dienste“ von Google Workspace for Education (wie YouTube und Suche).	Google ist ein Verarbeiter für die **Takeout-Tools** für Administratoren und Endnutzer geworden.
Keine Zweckbegrenzung ChromeOS und Browser	Unterzeichnen Sie die neue (niederländische) Vereinbarung für ChromeOS und Browser-Auftragsverarbeitung. Aktivieren Sie nicht die optionalen Chrome-Dienste, für die Google ein für die Datenverarbeitung Verantwortlicher bleibt (für	Der Auftragsverarbeitungsvertrag für das verwaltete ChromeOS und den Browser enthält zwei erschöpfende Listen von Zwecken, für Google als Auftragsverarbeiter und für die vereinbarte Weiterverarbeitung durch Google als für die Verarbeitung Verantwortlicher für seine eigenen legitimen Geschäftszwecke.

Maßnahmen für Administratoren von ChromeOS

Problem	Empfohlene Maßnahmen für Schulen	Durch Google getroffene Maßnahmen
	Neukunden bereits deaktiviert).	
	Wählen Sie die Einstellung K-12 (Alter) (auch Universitäten), um die Verarbeitung zu kommerziellen Zwecken zu blockieren, wie z. B. die Erstellung von Gruppenprofilen in der Privacy Sandbox und die Anzeige von Umfragen bei den Endnutzern durch Google.	
Keine Zweckbegrenzung Sync-Daten außerhalb von Workspace for Education	Obwohl die fehlende Zweckbegrenzung behoben wurde, ist Schulen noch immer zu empfehlen, Chrome Sync nicht zu aktivieren, wenn Nutzer Google-Konten für private Zwecke nutzen dürfen - wegen der Risiken einer Übertragung in Drittländer (siehe separate DTIA zu Google Meet). *DTIA = Data Transfer Impact Assessment; Folgenabschätzung zu Datentransfers*	Auf der Grundlage des Verarbeitungsvertrags für das verwaltete ChromeOS und den Browser ist Google ein Datenverarbeiter für Chrome Sync, sowohl für die Inhalte als auch für die Diagnosedaten (unabhängig von Workspace for Education, wo Google bereits als Verarbeiter für Sync fungiert.
Keine Zweckbegrenzung („verwalteter“) Play Store und Chrome Webstore	Deaktivieren Sie den Zugriff auf alle „zusätzlichen Dienste“ (Additional Services) in Google Workspace, einschließlich des (verwalteten) Play Store und des optionalen Dienstes (Optional Service) Chrome Webstore. Wenn Schulen ihren Schülern die Nutzung ausgewählter Apps ermöglichen wollen, sollten sie diese Apps über ihr eigenes Netzwerk verteilen. Bei Browsererweiterungen können sie die Zwangsinstallation (Force installation) anwenden, ohne dass die Nutzer den Chrome Webstore besuchen müssen.	Google hat bisher noch keine Maßnahmen angekündigt.

Maßnahmen für Administratoren von ChromeOS

Problem	**Empfohlene Maßnahmen für Schulen**	**Durch Google getroffene Maßnahmen**
Keine Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA und die Weiterübermittlung in 7 Drittländer	Unterzeichnen Sie die neue (niederländische) ChromeOS- und Browser-Auftragsverarbeiter-Vereinbarung einschließlich der neuen Standardvertragsklauseln (Standard Contractual Clauses, SCC) und wenden Sie alle Datenminimierungsmaßnahmen aus den aktualisierten (niederländischen) Leitlinien von SIVON an, einschließlich aller Schritte im (niederländischen) Leitfaden.	Google ist zum Auftragsverarbeiter für das verwaltete ChromeOS und den Browser geworden, [vertrauliche Informationen wurden aus dieser öffentlichen Tabelle entfernt].
	Deaktivieren Sie SafeSites mit einer Registry-Einstellung (erwägen Sie die Verwendung eines Filters eines Drittanbieters).	Google reagierte nicht auf die Aufforderung, eine lokale Filterung zuzulassen, anstatt die URLs mit den IP-Adressen in die USA zu übermitteln.
	Setzen Sie alle empfohlenen datenschutzfreundlichen Einstellungen zentral durch, einschließlich der Deaktivierung des Zugriffs auf google.com und youtube.com, entweder indem Sie die Verwendung eines Proxy-Servers zur Blockierung von Funktionen im lokalen Netzwerk erzwingen oder über manuelle URL-Blockierungsmöglichkeiten im Admin-Portal.	Google stellt zentrale Verwaltungsoptionen für den Gastmodus auf verwalteten Chromebooks bereit, einschließlich der Blockierung von Cookies von Drittanbietern.
	Schulen wird (weiterhin) davon abgeraten, Chrome Sync zu aktivieren, wenn die Nutzer Google-Konten für private Zwecke nutzen dürfen, einschließlich privater E-Mails und privatem Surfverhalten, aus denen	Google überträgt die personenbezogenen Daten an 7 Drittländer. Aus der für Google Workspace Meet durchgeführten DTIA geht hervor, dass die Übertragung besonderer Kategorien personenbezogener Daten zu

Maßnahmen für Administratoren von ChromeOS

Problem	Empfohlene Maßnahmen für Schulen	Durch Google getroffene Maßnahmen
	besondere Kategorien personenbezogener Daten abgeleitet werden können - wegen des Risikos eines unbefugten Zugriffs durch staatliche Stellen in Drittländern.	einem hohen Risiko führt, wenn Schulen diese Daten nicht mit einem lokal gespeicherten Schlüssel verschlüsseln können.
	Deaktivieren Sie Sync, indem Sie die Richtlinie SyncDisabled auf true setzen, oder stellen Sie sicher, dass die Schüler eine selbst verwaltete lokale Passphrase zur Verschlüsselung der Sync-Daten verwenden.	Google hat noch keine Richtlinien für Administratoren entwickelt, um die Verwendung der Chrome Sync-Datenverschlüsselung mit lokal verwalteten Schlüsseln auf den Geräten der Endnutzer zentral durchzusetzen. *Gemeint sein dürfte hier die Client-seitige Verschlüsselung.*
Datenschutzunfreundliche Standardeinstellungen	Erzwingen Sie, wo immer möglich, die empfohlenen datenschutzfreundlichen Einstellungen.	Privacy Sandbox-Tests sind für Benutzer unter 18 Jahren deaktiviert (K-12).
		Google hat nicht auf die Aufforderung reagiert, die Funktionen zum Schutz vor Tracking im Chrome-Browser zu verbessern, wenn Cookies von Drittanbietern blockiert sind, das DNT-Signal aktiviert ist und das Website-Preloading deaktiviert ist. Zum Beispiel durch Blockieren des Datenverkehrs zu Google-Diensten, bei denen Google nicht als Auftragsverarbeiter fungiert (wie Analytics und Schriftarten).
	Deaktivieren Sie die Privacy Sandbox für alle Benutzer (ist bereits deaktiviert, wenn Schulen dem Rat folgen, die Einstellung K-12 zu wählen).	Google hat Administratoren die Möglichkeit gegeben, die Personalisierung und Messung von Werbung im Rahmen der Privacy Sandbox in der Auftragsverarbeiter-Version

Maßnahmen für Administratoren von ChromeOS

Problem	Empfohlene Maßnahmen für Schulen	Durch Google getroffene Maßnahmen
		des verwalteten ChromeOS zu blockieren.
Mangel an Transparenz	Sperren Sie weiterhin zentral den Zugriff auf den Chrome Web Store und den Google Play Store.	Google hat bisher keine Maßnahmen angekündigt.

Hinweis: Das ursprüngliche Dokument stammt aus
https://www.surf.nl/files/2024-06/verification-report-processor-version-google-chrome-for-education-7-march-2024.pdf

Die beiden Texte in der Tabelle im folgenden Format sind Ergänzungen/ Kommentare des Übersetzers: *Data*