Google Cloud Whitepaper
Dezember 2020

# Google Workspace Leitfaden zur Umsetzung des Datenschutzes

Google Cloud

# Inhalt



## *Haftungsausschluss*

Dieser Leitfaden ist für Google Workspace-Administratoren bestimmt und erläutert, wie sie Google Workspace-Dienste und -Einstellungen verwenden und individuell einrichten können, um datenschutzrechtliche Anforderungen einzuhalten. Sie sollten einen Rechtsexperten hinzuziehen, um sich zu den besonderen Anforderungen beraten zu lassen, die für ihre Organisation gelten, denn dieser Leitfaden ist nicht als Rechtsberatung zu verstehen.

Der Inhalt des Leitfadens ist auf dem Stand von Dezember 2020 und entspricht dem Status quo zum Zeitpunkt der Erstellung. Die Richtlinien und Systeme von Google können sich in Zukunft ändern, denn wir optimieren den Schutz für unsere Kunden ständig.

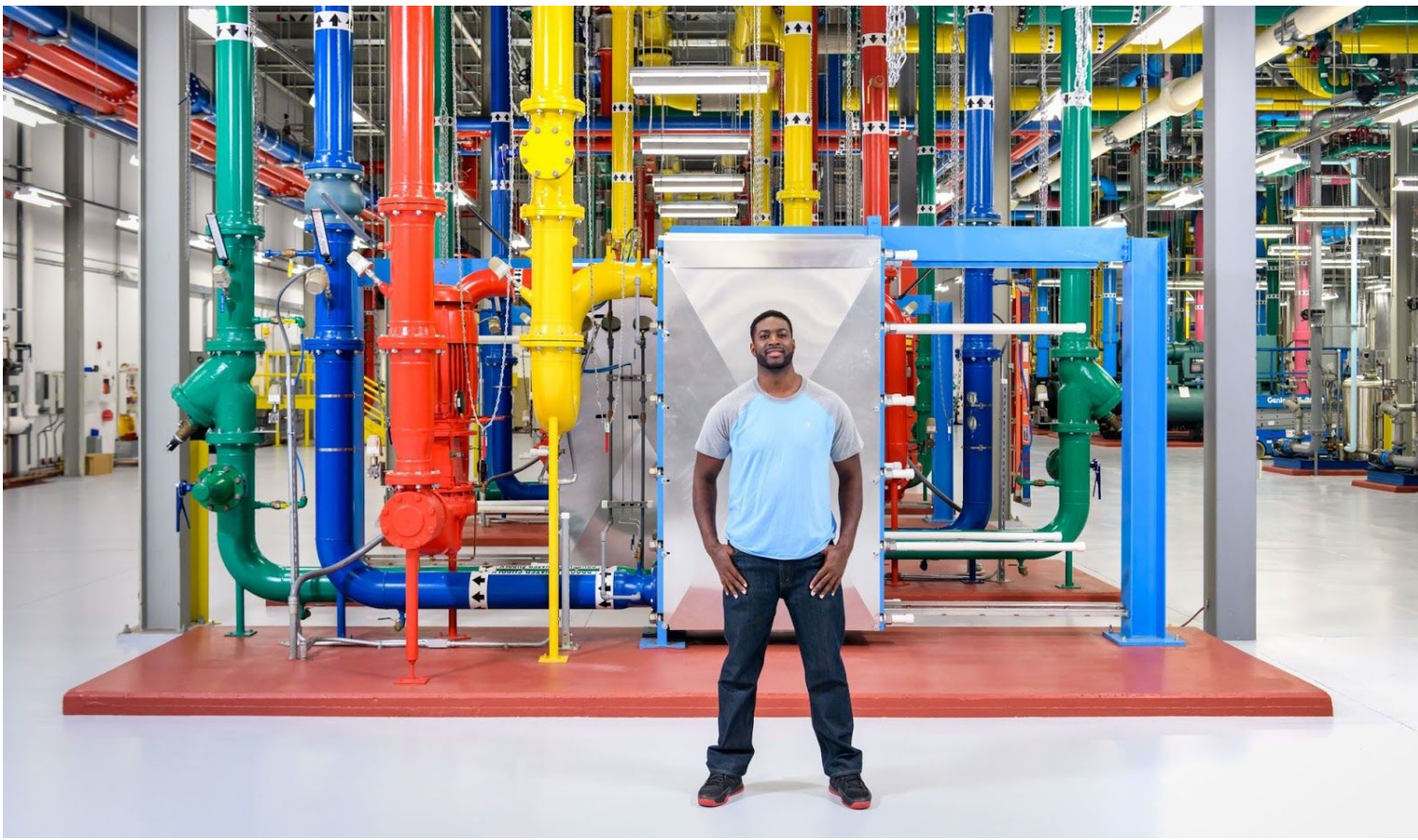
# Verarbeitung personenbezogener Kundendaten im Rahmen unserer Dienste

## Die richtigen Maßnahmen für Ihre Datenschutzanforderungen

Wir sehen es als unsere Aufgabe an, unsere Kunden bei der Einhaltung ihrer Datenschutzverpflichtungen zu unterstützen, einschließlich der Bestimmungen der EU-Datenschutz-Grundverordnung (DSGVO). Deshalb stellen wir ihnen nützliche Produkte und Tools zur Verfügung, binden bewährte Datenschutz- und Sicherheitsmaßnahmen in unsere Dienste und Verträge ein und legen Zertifizierungen und Auditberichte vor.

Im Zusatz zur Datenverarbeitung von Google Workspace ist Google als Auftragsverarbeiter der personenbezogenen Kundendaten genannt, die über die Google Workspace-Dienste eingereicht, gespeichert, gesendet oder von Ihrer Organisation erhalten werden. Wir verarbeiten diese Daten in Ihrem Namen und gemäß Ihren Anweisungen. Als Kunde gelten Sie als Verantwortlicher für die personenbezogenen Kundendaten[1]. Das bedeutet, Sie entscheiden über die Zwecke und Mittel der Verarbeitung.

Sie sollten sich die Google Workspace-Vereinbarung und den Zusatz zur Datenverarbeitung von Google Workspace genau ansehen. Dies gilt ebenso für die Nutzungsbedingungen anderer Google-Dienste, die Sie Ihren Endnutzern bei der Anmeldung in von der Organisation verwalteten Konten zur Verfügung stellen möchten, beispielsweise die für Ihre Domain aktivierten zusätzlichen Dienste.



## Unsere Selbstverpflichtung zum Datenschutz

Die Selbstverpflichtungen zum Datenschutz für Unternehmen geht Google für Google Workspace-Produkte im Rahmen seiner übergeordneten Verantwortung ein, Unternehmen bei der Nutzung seiner Lösungen zu schützen. Diese Selbstverpflichtungen ergänzen die strengenvertraglichen Verpflichtungen, die Google Ihnen gegenüber eingeht.

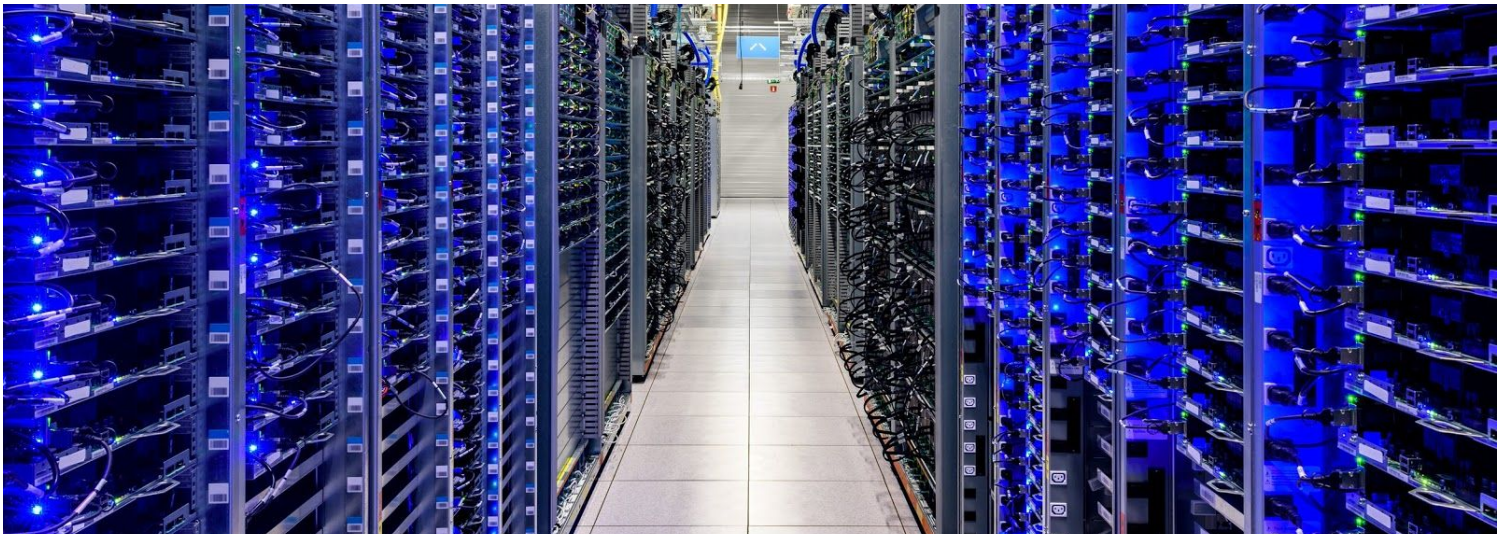
- **Sie haben die Kontrolle über Ihre Daten.** Kundendaten[2] gehören Ihnen und nicht Google. Wir verarbeiten Ihre Daten nur gemäß den mit Ihnen geschlossenen Vereinbarungen.
- **Wir verwenden Ihre Daten niemals zur Ausrichtung von Anzeigen.** Wir verarbeiten Ihre Kunden- oder Dienstdaten nicht, um Anzeigenprofile zu erstellen oder Google Ads-Produkte zu verbessern.
- **Wir gehen bei der Erhebung und Nutzung von Daten transparent vor.** Wir verpflichten uns zur Transparenz, zur Einhaltung von Vorschriften wie der DSGVO und zur Verwendung von Best Practices zum Datenschutz.
- **Wir verkaufen niemals Kunden- oder Dienstdaten.** Wir verkaufen Kundendaten oder Dienstdaten[3] niemals an Dritte.
- **Sicherheit und Datenschutz haben bei allen unseren Produkten höchste Priorität.** Die Privatsphäre unserer Kunden liegt uns am Herzen. Daher ist uns der Schutz der uns anvertrauten Daten äußerst wichtig und wir binden die stärksten Sicherheitstechnologien in unsere Produkte ein.

Google Workspace wurde unter Einhaltung rigoroser Datenschutz- und Sicherheitsstandards entwickelt, die auf branchenüblichen Best Practices basieren.[4] Zusätzlich zu unseren strengen vertraglichen Verpflichtungen hinsichtlich Eigentum, Verwendung, Sicherheit und Transparenz der Daten sowie der damit verbundenen Rechenschaftspflicht stellen wir Ihnen die Tools zur Verfügung, die Sie zur Erfüllung der Anforderungen an Compliance und Berichterstellung benötigen. Weitere Informationen finden Sie in Anhang 1. Darüber hinaus bieten unsere Vertrauensgrundsätze Klarheit über unsere Selbstverpflichtung zum Datenschutz und machen deutlich, was Sie in Bezug auf den Schutz und die Verwaltung Ihrer Daten in der Cloud erwarten können.

Transparenz gehört zu unseren Grundsätzen. Wir setzen alles daran, durch Transparenz das Vertrauen unserer Kunden zu gewinnen und zu erhalten. Wir bei Google Cloud sind überzeugt, dass Vertrauen durch Transparenz geschaffen wird. Wir möchten nicht nur transparent sein, was unsere Selbstverpflichtungen betrifft, sondern auch bezüglich dessen, was Sie erwarten können, wenn es um die gemeinsame Verantwortung für den Schutz und die Verwaltung Ihrer Daten in der Cloud geht. Unser Ziel ist, eine vertrauenswürdige Umgebung zu schaffen, indem wir uns auf drei Kernbereiche konzentrieren: Sicherstellung des Datenschutzes und der Sicherheit unserer Kundendaten, die Zuverlässigkeit unserer Dienste sowie die Festlegung und Einhaltung höchster Branchenstandards für Transparenz und Sicherheit.

Außerdem sorgen wir auch für die Sicherheit von Dienstdaten. Dienstdaten sind die Informationen, die Google bei der Bereitstellung und Verwaltung von Google Workspace erhebt oder erstellt und die für die Sicherheit und Verfügbarkeit unserer Dienste entscheidend sind. Kundendaten gehören nicht zu den

Dienstdaten. Als Dienstdaten zählen Informationen zu Sicherheitseinstellungen sowie Betriebs- und Abrechnungsdaten. Wir verarbeiten Dienstdaten für verschiedene Zwecke, die in unseren neu veröffentlichten Google Cloud-Datenschutzhinweisen im Detail genannt sind. Dazu gehören unter anderem Empfehlungen zur Optimierung Ihrer Nutzung von Google Workspace und zur Verbesserung von Leistung und Funktion.

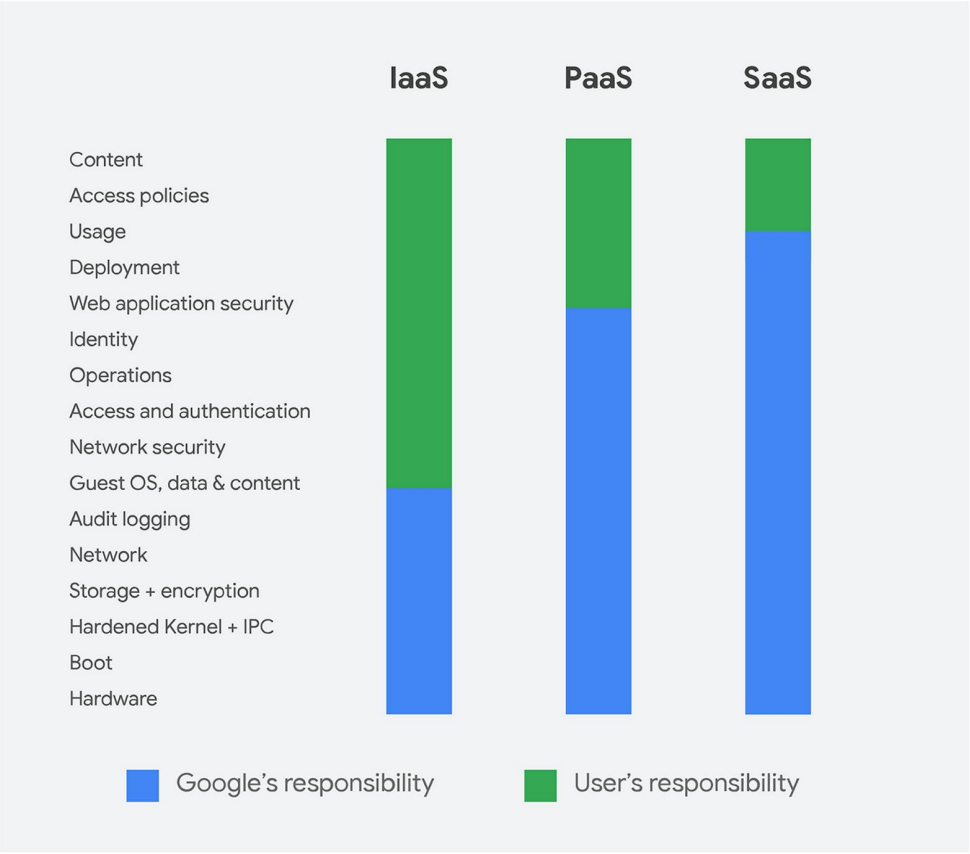


## Unser Modell der geteilten Verantwortung

Datenschutz ist nicht nur die Verantwortung des Unternehmens, das die Google Workspace-Dienste verwendet, und obliegt auch nicht allein Google bei der Bereitstellung dieser Dienste. Datenschutz in der Cloud ist stattdessen eine geteilte Verantwortung: eine gemeinschaftliche Aufgabe von Kunde und Cloud-Dienstanbieter.

Das Modell der geteilten Verantwortung von Google ist eine visuelle Darstellung der verschiedenen Sicherheitszuständigkeiten, für die der Kunde und Google gemeinsam die Verantwortung tragen. Google Workspace ist eine Software as a Service (SaaS), bei der fast alles bis auf die Inhalte und die Zugriffsregelung der Verantwortung des Cloud-Dienstanbieters unterliegt. Im SaaS-Modell verwalten Cloud-Dienstanbieter die gesamte physische und virtuelle Infrastruktur und die Plattformebene und stellen cloudbasierte Anwendungen/Apps und Dienste zur Nutzung durch den Kunden bereit. Internetanwendungen, die direkt in einem Webbrowser ausgeführt werden, und mobile Apps sind SaaS-Anwendungen. Mit diesem Modell müssen sich Kunden bei Anwendungen nicht um die Installation, Aktualisierung oder den Support kümmern, sondern nur Systeme und Datenzugriffsregelungen verwalten.

**Wichtig:** Als Google Workspace-Kunde sind Sie für die Sicherheit aller Komponenten verantwortlich, die Sie zur Verfügung stellen oder die Ihrer Kontrolle unterliegen, beispielsweise für die Inhalte, die Sie in die Google Workspace-Dienste stellen, sowie für die Einrichtung einer Zugriffssteuerung für Ihre Nutzer.




Das Modell der geteilten Verantwortung kann als Anleitung dafür dienen, wie Sie Ihre Kundendaten auf Google Workspace schützen können. Unter verschiedenen Datenschutzvorschriften sind Sie dafür verantwortlich, Sicherheitsvorkehrungen zum Schutz der personenbezogenen Kundendaten in Ihrem Besitz zu ergreifen, die Verarbeitung der personenbezogenen Kundendaten zu beaufsichtigen, die Richtigkeit der Daten sicherzustellen und den Lebenszyklus der Daten zu verwalten.

Google schützt die Google Workspace zugrundeliegende Infrastruktur während des gesamten Zyklus der Informationsverarbeitung. Dank Hardwareschicht, Kommunikation zwischen Diensten, Zugriffsverwaltung zwischen Diensten, Datenspeicherung, Kommunikation über das Internet und Betriebssicherheit wird auf jeder Ebene für Sicherheit gesorgt. Weitere Informationen zu diesem Thema finden Sie im Whitepaper Übersicht über das Sicherheitsdesign der Infrastruktur von Google.

# Google-Dienste

In diesem Abschnitt finden Sie einen Überblick über die Google-Dienste, darunter die Google Workspace-Hauptdienste, eingebettete Funktionen, zusätzliche Dienste, von der Organisation verwaltete Google-Konten und technische Supportdienste.

- **Google Workspace-Hauptdienste**: die in der Zusammenfassung der Dienste genannten und beschriebenen Dienste.
- **In Google Workspace-Hauptdienste eingebettete Funktionen**: in die Google Workspace-Hauptdienste eingebunden und automatisch für alle Google Workspace-Nutzer verfügbar.
- **Feedback**: Feedback zu vorgeschlagenen Rechtschreib- und Grammatikkorrekturen sowie in den Produkten unterliegt der Datenschutzerklärung von Google.
- **Zusätzliche Dienste**: Zusätzliche Dienste werden nicht als Bestandteil von Google Workspace verkauft. Hierbei kann es sich um Google-Dienste handeln, die mit einem von der Organisation verwalteten Google-Konto verwendet werden können. Eine unvollständige Liste zusätzlicher Google-Dienste finden Sie hier.
- **Von der Organisation verwaltetes Google-Konto**: Sie können Google Workspace nur mit einem von der Organisation verwalteten Google-Konto verwenden, also einem Konto, das von Ihrem perivaten Google-Konto getrennt ist. Dieses Konto wird von einem Administrator verwaltet.
- **Technische Supportdienste**: Google Workspace-Administratoren können sich per Telefon, E-Mail oder Chat an Google wenden, um technischen Support zu erhalten.

## Google Workspace-Hauptdienste

Zu den Hauptdiensten von Google Workspace gehören die Dienste, die in der Dienstübersicht der Nutzungsbedingungen für Google Workspace beschrieben sind, beispielsweise Gmail, Google Docs, Google Tabellen und Google Präsentationen. Das sind die Dienste, die Google Workspace-Kunden im Rahmen ihrer Google Workspace-Vereinbarung nutzen können.[5]

Im Zusatz zur Datenverarbeitung für Google Workspace ist festgelegt[6], wie Google die Kundendaten seiner Hauptdienste verarbeitet. Kundendaten sind die Daten, die Organisationen und ihre Nutzer an Google zur Verarbeitung in den Google Workspace-Hauptdiensten weitergeben, einschließlich personenbezogener Kundendaten (gemäß der Definition im Zusatz zur Datenverarbeitung). Kunden können dem Zusatz zur Datenverarbeitung in der Google Admin-Konsole zustimmen, wenn sie sich außerhalb Europas befinden und der Ansicht sind, dass dieser ihren Compliance-Anforderungen entspricht.

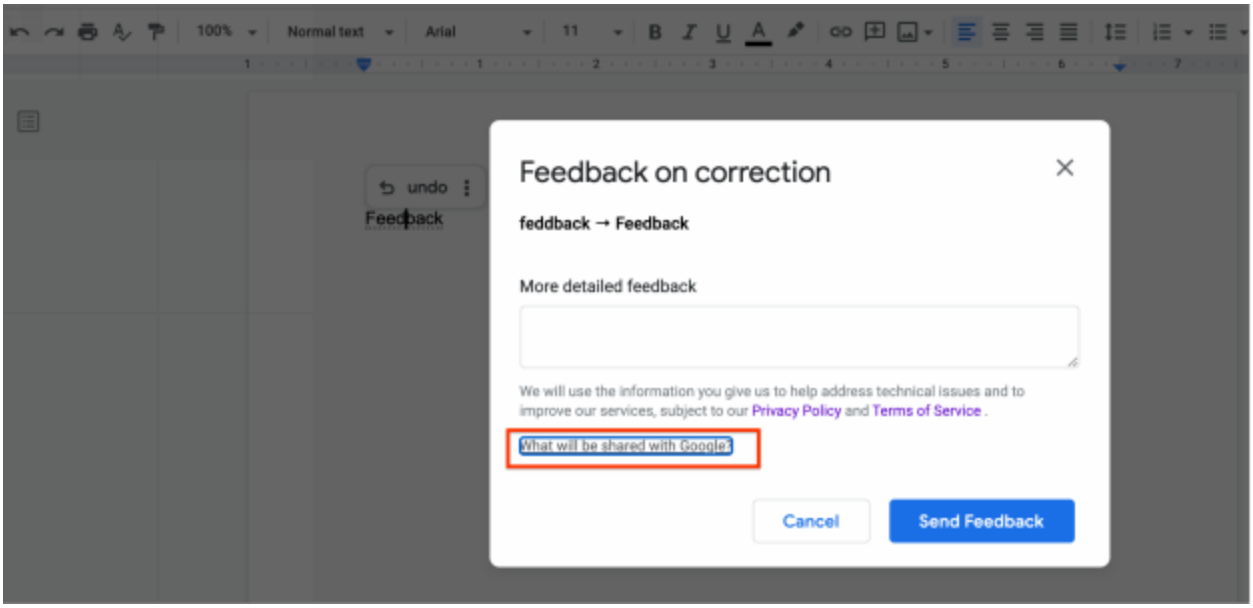
## In Google Workspace-Hauptdienste eingebettete Funktionen

Zu den Hauptdiensten gehören verschiedene Funktionen wie die Rechtschreib- und Grammatikprüfung, Erkunden, Integration der Kalender-Standortbestimmung und Google Übersetzer. Diese Funktionen sind in den Google Workspace-Hauptdiensten eingebettet und automatisch für alle Google Workspace-Nutzer verfügbar. Google ist ein Datenauftragsverarbeiter für personenbezogene Kundendaten, die über die eingebetteten Funktionen in den Google Workspace-Hauptdiensten verarbeitet werden. Bei Verwendung mit den Google -Hauptdiensten unterliegen die Funktionen dem Zusatz zur Datenverarbeitung für Google Workspace.

Die Nutzer können einige eingebettete Funktionen deaktivieren (sie können beispielsweise die Autokorrektur und die Vorschläge unter Rechtschreibung und Grammatik in Google Docs und Gmail deaktivieren) oder sich dafür entscheiden, die eingebetteten Funktionen nicht zu verwenden (beispielsweise „Dokument übersetzen“ und „Erkunden“). Wenn Sie die Funktion „Erkunden“ zum Aufrufen der Website eines Drittanbieters verwenden, unterliegt die Nutzung dieser Website nicht dem Zusatz zur Datenverarbeitung für Google Workspace.

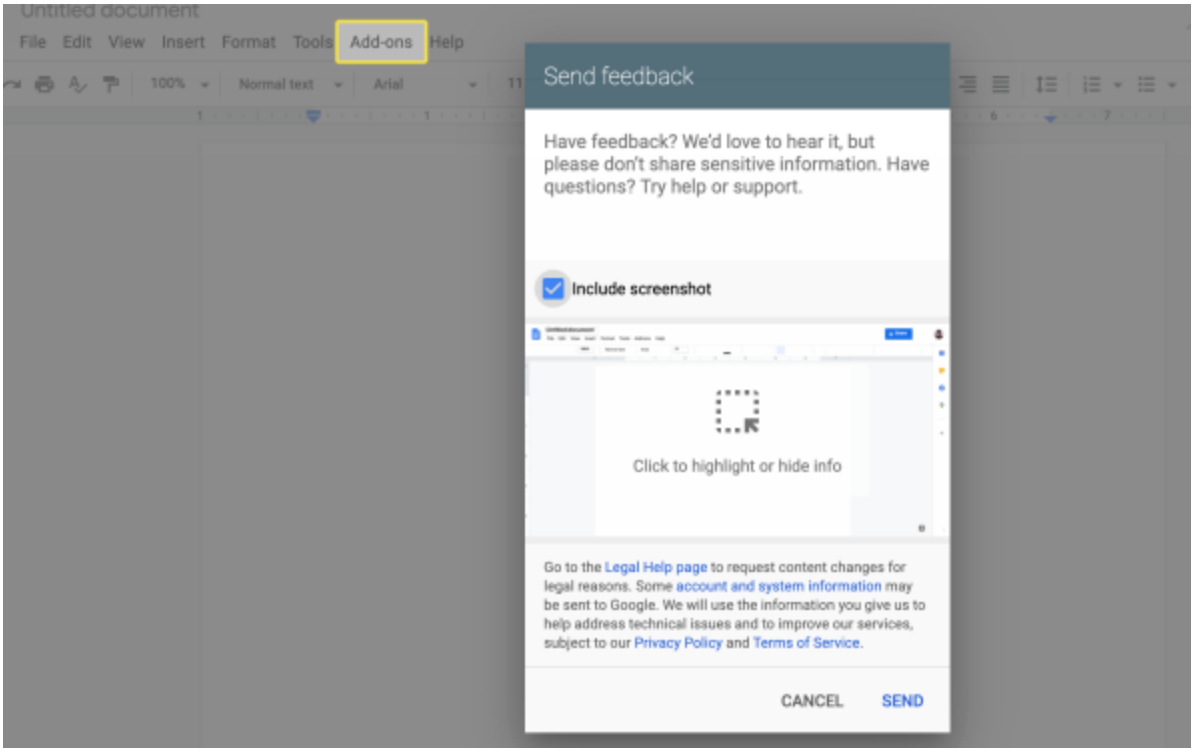
## Feedback

Nutzer können Feedback zu vorgeschlagenen Rechtschreib- und Grammatikkorrekturen geben (siehe Beispiel unten). Bitte beachten Sie, dass Ihre Kundendaten nicht zur Verbesserung der Rechtschreib- und Grammatikdienste für andere Kunden verwendet werden.




Wir bieten den Nutzern auch die Option Feedback im Produkt zu geben. Sie haben die Möglichkeit, Screenshots zu einem Problem zu senden und wir stellen ein Tool zum Ausblenden vertraulicher Informationen bereit. **Feedback, das freiwillig über unsere Feedback-Tools gegeben wird, wird gemäß**

**der Datenschutzerklärung von Google verarbeitet. Wir informieren die Nutzer vor dem Senden des Feedbacks über diese Bestimmungen.** Google fungiert als Verantwortlicher für das Feedback, das wir zu Rechtschreib- und Grammatikkorrekturen sowie in den Produkten erhalten.




## Zusätzliche Dienste

Zusätzliche Dienste werden nicht als Bestandteil von Google Workspace verkauft. Hierbei kann es sich um Google-Dienste handeln, die mit einem von der Organisation verwalteten Google-Konto verwendet werden können. Eine unvollständige Liste zusätzlicher Google-Dienste finden Sie hier. **Diese Dienste und Produkte gehören nicht zu Google Workspace und unterliegen deshalb weder dem Zusatz zur Datenverarbeitung für Google Workspace noch der Google Workspace-Vereinbarung**.

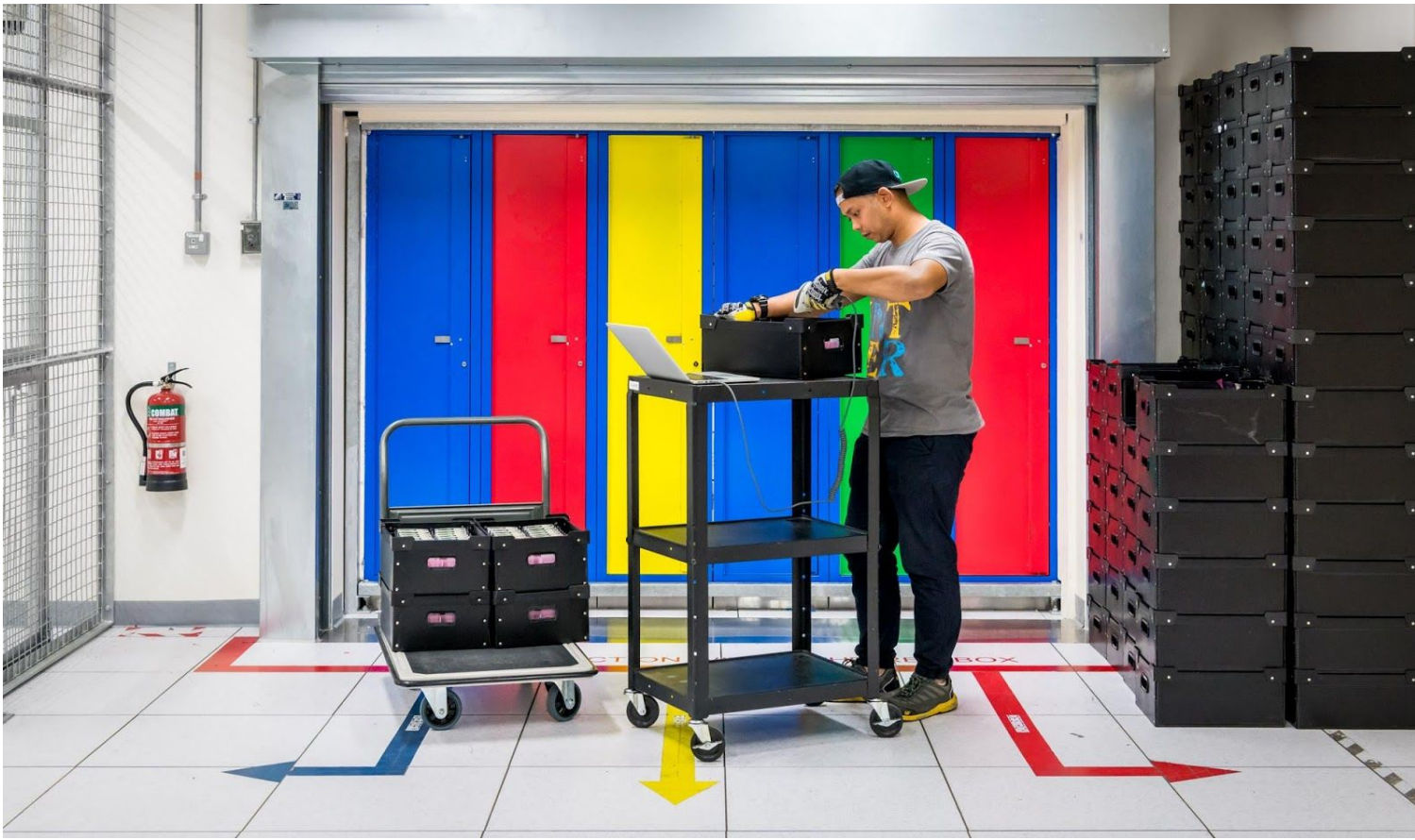
Die Nutzer von Google Workspace-Kunden können jedoch über ihre von der Organisation verwalteten Google-Konten auf die zusätzlichen Dienste zugreifen. Wie auf der Seite Zusätzliche Google-Dienste beschrieben, unterliegen die meisten zusätzlichen Dienste den Nutzungsbedingungen und der Datenschutzerklärung von Google. Für einige dieser Dienste gibt es außerdem eigene Nutzungsbedingungen. Sie finden diese Bedingungen unter Zusätzliche Google-Dienste im Abschnitt mit der Überschrift *Dienste, die Sie einzeln aktivieren oder deaktivieren können*.

**Wichtiger Hinweis:** Google Workspace-Administratoren müssen den Zugriff ihrer Nutzer auf die zusätzlichen Dienste aus Compliance-Gründen möglicherweise einschränken, wenn diese in ihrem von der Organisation verwalteten Google-Konto angemeldet sind.

Administratoren (auch als *Admins* bezeichnet) können festlegen, auf welche zusätzlichen Dienste die Nutzer zugreifen dürfen, wenn sie in ihrem von der Organisation verwalteten Google-Konto angemeldet sind, indem sie die Dienste für die Nutzer in der Google Admin-Konsole einzeln *aktivieren* oder *deaktivieren*. Der Administrator kann diese Einstellungen konfigurieren, bevor er ein Nutzerkonto einrichtet. Eine Anleitung finden Sie unter Zusätzliche Google-Dienste im Abschnitt mit der Überschrift *Dienste für Nutzer aktivieren oder deaktivieren*. Neben Google Workspace und anderen Diensten von Google, die Admins einzeln in der Admin-Konsole verwalten können, haben sie auch die Möglichkeit, den Zugriff auf nicht gelistete Google-Dienste einzuschränken, die sich nicht einzeln verwalten lassen, beispielsweise Chromecast und Google Surveys. Weitere Hinweise zur Aktivierung oder Deaktivierung dieser Dienste finden Sie in diesem Hilfeartikel.

**Hinweis:** Nutzer, die nicht in ihrem von der Organisation verwalteten Google-Konto angemeldet sind, können zusätzliche Dienste verwenden, auch wenn der Google Workspace-Administrator den Zugriff auf diese Dienste für angemeldete Nutzer deaktiviert hat. Wenn der Administrator in der Admin-Konsole beispielsweise YouTube für die Organisation deaktiviert hat, können nicht angemeldete Nutzer YouTube trotzdem verwenden. In diesem Fall verarbeitet Google keine Daten, die mit dem von der Organisation verwalteten Google-Konto des Nutzers verknüpft sind.

Der Rechtsberater oder Datenschutzbeauftragte (DSB) Ihrer Organisation bzw. jemand in ähnlicher Funktion sollte eine Datenschutz-Folgenabschätzung für die Verarbeitung der personenbezogenen Kundendaten aus diesen Produkten durchführt, um festzustellen, ob und wie Ihre Organisation ihre Verpflichtungen als Datenverantwortlicher bzw. Datenauftragsverarbeiter für jedes dieser Produkte erfüllen kann.



## Von der Organisation verwaltete Google-Konten

Nutzer in Ihrer Organisation können die Google Workspace-Dienste nur verwenden, wenn sie jeweils ein eigenes Google-Konto haben. Mit einem von der Organisation verwalteten Google-Konto werden jedem Nutzer ein Name und ein Passwort für die Anmeldung in den Google-Diensten, eine E-Mail-Adresse in Ihrer Domain sowie ein Profil zugewiesen. Informationen wie Name oder Profilbild können von den Nutzern selbst angegeben werden. Daten dazu, wann, wofür und in welchem Kontext (App/Web, Plattform und Gerät) sich ein Nutzer anmeldet, erhebt Google automatisch. Meldet sich ein Nutzer zum ersten Mal in seinem von der Organisation verwalteten Google-Konto an, wird er in einer Mitteilung darüber informiert, wie seine Daten erhoben werden und wie der Administrator darauf zugreift. Außerdem wird darauf hingewiesen, dass die Verwendung der Google Workspace-Hauptdienste den Nutzungsbedingungen für Google Workspace Ihrer Organisation unterliegt. Weiterhin wird erläutert, dass die Verwendung der zusätzlichen Dienste in Verbindung mit dem von der Organisation verwalteten Google-Konto der Datenschutzerklärung und den Nutzungsbedingungen von Google sowie den geltenden dienstspezifischen Nutzungsbedingungen unterliegt. Weitere Informationen dazu, wie Sie von der Organisation verwaltete Google-Konten erstellen, finden Sie im Hilfeartikel Optionen zum Hinzufügen von Nutzern.

## Technische Supportdienste

Google Workspace-Administratoren können zwischen Online-, Telefon- und Chatsupport wählen. Daten, die im Rahmen der Bereitstellung technischer Supportdienste für Ihre Nutzung der Google Workspace-Hauptdienste erhoben und verarbeitet werden, unterliegen den Richtlinien für technische Supportdienste von Google Workspace und den Google Cloud-Datenschutzhinweisen. Google erhebt und verarbeitet die benötigten Daten zur Bereitstellung und Verwaltung der in diesen Richtlinien beschriebenen Supportdienste. Google ist gemäß der Google Workspace-Vereinbarung oder den Richtlinien für technische Supportdienste nicht verpflichtet, Supportleistungen für zusätzliche Dienste zu erbringen.

# Best Practices für den Datenschutz

In diesem Abschnitt stellen wir einige Best Practices dazu vor, wie Sie die Google Workspace-Dienste an die Datenschutzanforderungen Ihrer Organisation anpassen können. Bitte beachten Sie, dass es sich nicht um eine vollständige Liste aller Best Practices handelt. Außerdem ist dieser Leitfaden nicht als Rechtsberatung zu verstehen. Am besten besprechen Sie mit einem Rechtsexperten oder dem Datenschutzbeauftragten Ihrer Organisation, welche speziellen Anforderungen für Ihre Organisation gelten.

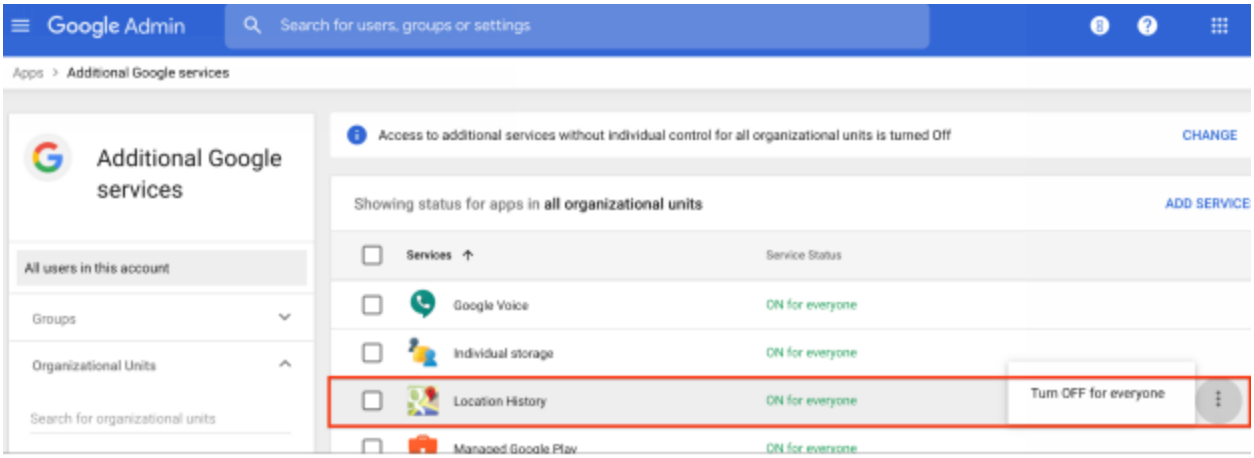
## Zusätzliche Dienste für Nutzer auswählen

Zusätzliche Dienste sind nicht im Google Workspace-Angebot enthalten und unterliegen weder dem Zusatz zur Datenverarbeitung für Google Workspace noch der Google Workspace-Vereinbarung. In der Admin-Konsole sind alle zusätzlichen Dienste standardmäßig aktiviert. Wir empfehlen Administratoren, eine sorgfältige Auswahl zu treffen, welche zusätzlichen Dienste (beispielsweise YouTube, Maps oder Blogger) für ihre Nutzer aktiviert/deaktiviert werden sollen, insbesondere für Kunden mit Altersbeschränkungen oder Kunden, die streng regulierte oder sensible Daten verarbeiten (beispielsweise Finanzdaten, Gesundheitsdaten und Behördendaten). Weitere Informationen hierzu finden Sie im Abschnitt „Zusätzliche Dienste“ in diesem Leitfaden.

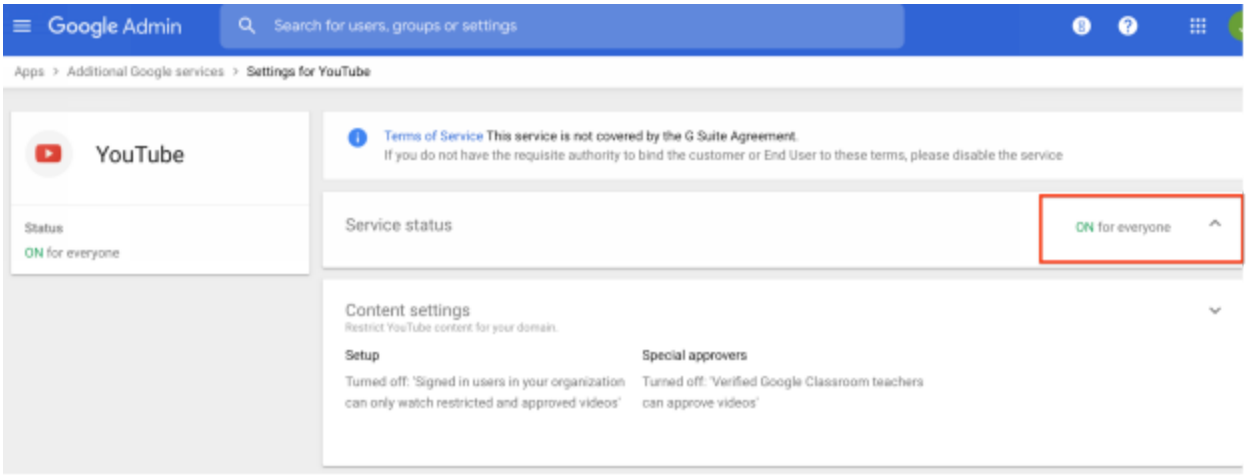
## Nutzer beim Festlegen der Aktivitätseinstellungen zum Schutz ihrer Privatspähre unterstützen

Empfehlen Sie den Nutzern, nur den Aktivitätseinstellungen zuzustimmen, die den Datenschutzrichtlinien Ihres Unternehmens und ihren persönlichen Anforderungen entsprechen. Google speichert Aktivitäten, um die Verwendung seiner Dienste zu personalisieren und zu optimieren. Wenn Nutzer das für ihr von der Organisation verwaltetes Konto nicht möchten, zeigen Sie ihnen, wie sie bestimmte Einstellungen auf der Seite Aktivitätseinstellungen deaktivieren können. Die folgenden Anleitungen und Richtlinien enthalten weitere Informationen.

- **Standortverlauf**: Überlegen Sie, ob Sie den Standortverlauf für die von der Organisation verwalteten Google-Konten Ihrer Nutzer aktivieren oder deaktivieren möchten. Standardmäßig ist der Standortverlauf für die Nutzer **deaktiviert**. Möchten Sie das ändern, muss die Einstellung von Ihnen in der Google Admin-Konsole **und** von den Nutzern aktiviert werden. Gehen Sie in der Admin-Konsole zu *Apps* > *Zusätzliche Google-Dienste* > *Standortverlauf*. Die Nutzer können den Standortverlauf auf der Seite Aktivitätseinstellungen ihres von der Organisation verwalteten Google-Kontos aktivieren oder deaktivieren. Eine Anleitung für Nutzer finden Sie im Hilfeartikel Standortverlauf verwalten.

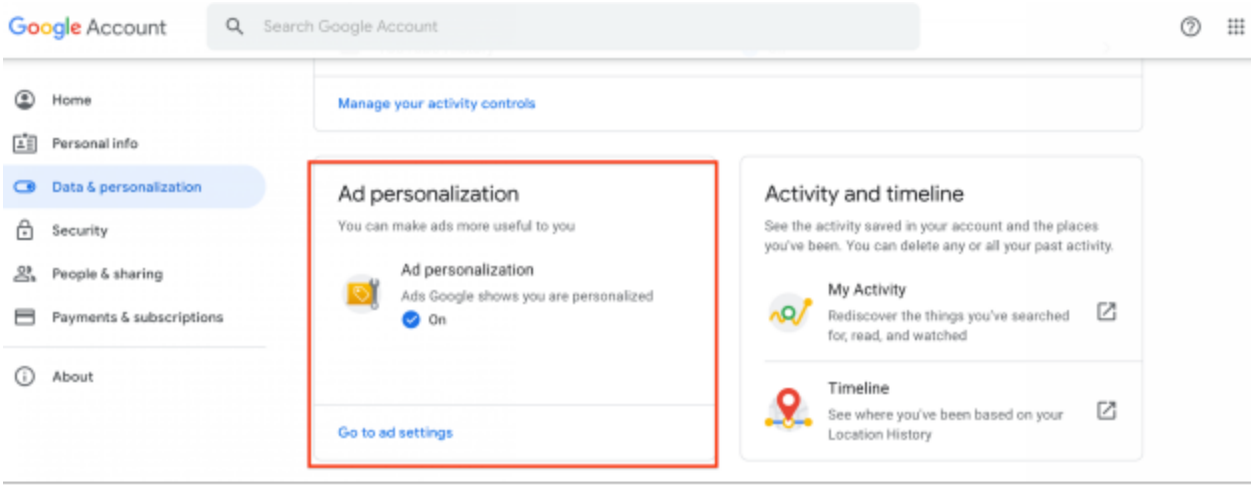



- **YouTube-Verlauf**: Überlegen Sie, ob Sie YouTube für Ihre Nutzer aktivieren oder deaktivieren möchten. Gehen Sie in der Admin-Konsole zu *Apps* > *Zusätzliche Google-Dienste* > *YouTube*, um den YouTube-Verlauf zu aktivieren. Anschließend können die Nutzer den **YouTube-Verlauf** auf der Seite Aktivitätseinstellungen für sich aktivieren oder deaktivieren. Bei deaktiviertem Verlauf werden angesehene Videos nicht gespeichert und der Verlauf wird nicht zur Verbesserung von Empfehlungen verwendet. Eine Anleitung für Nutzer finden Sie im Hilfeartikel Wiedergabeverlauf aufrufen, löschen oder pausieren



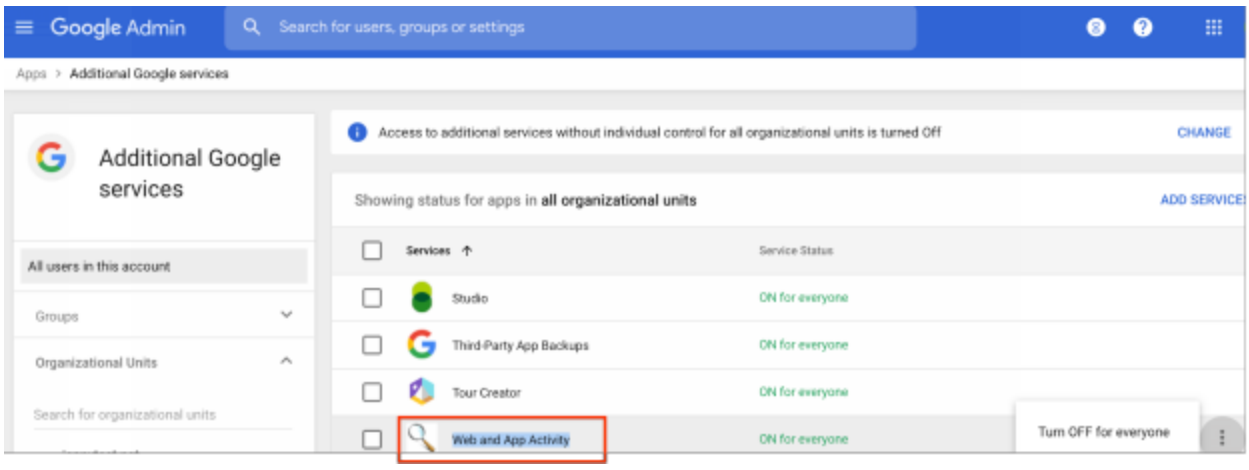

- **Personalisierte Werbung**: Bei der Anzeigenbereitstellung werden personenbezogene Daten im von der Organisation verwalteten Google-Konto des Nutzers ebenso berücksichtigt wie Daten von Werbetreibenden, die mit Google zusammenarbeiten, und Interessen, die Google bei dem Nutzer vermutet. Wenn personalisierte Werbung aktiviert ist, sehen Nutzer auf ihre Interessen zugeschnittene Werbeanzeigen. Auch diese Einstellung können die Nutzer auf der Seite Aktivitätseinstellungen steuern. Wenn personalisierte Werbung deaktiviert ist, verwendet Google die Nutzerinformationen nicht zur Personalisierung von Werbung. Eine Anleitung für Nutzer finden Sie im Hilfeartikel Eingeblendete Werbung anpassen.

  **Hinweis:** Google Workspace-Kundendaten werden von Google nicht für Werbezwecke verwendet. Personalisierte Werbung betrifft nur Google-Dienste, die nicht in Google Workspace enthalten sind.




- **Web- & App-Aktivitäten**: Überlegen Sie, ob Sie diese Einstellung für Nutzer aktivieren oder deaktivieren möchten. Gehen Sie in der Admin-Konsole zu *Apps > Zusätzliche Google-Dienste > Web- & App-Aktivitäten*. Standardmäßig ist die Einstellung für Ihre Organisation aktiviert, für die einzelnen Nutzer jedoch deaktiviert. Die Nutzer können die Einstellung aber selbst aktivieren. Wenn Sie die Option in der Admin-Konsole**deaktivieren**, haben die Nutzer diese Möglichkeit nicht.

  Wenn ein Nutzer die Einstellung „Web- & App-Aktivitäten“ aktiviert, werden seine Suchanfragen und Aktivitäten in anderen Google-Diensten in seinem von der Organisation verwalteten Google-Konto gespeichert. So profitiert er von personalisierten Suchergebnissen. Nutzer können ihre Web- und App-Aktivitäten auf der Seite Aktivitätseinstellungen aufrufen und löschen. Eine Anleitung dazu finden Sie unter „Web- & App-Aktivitäten“ ansehen und verwalten.

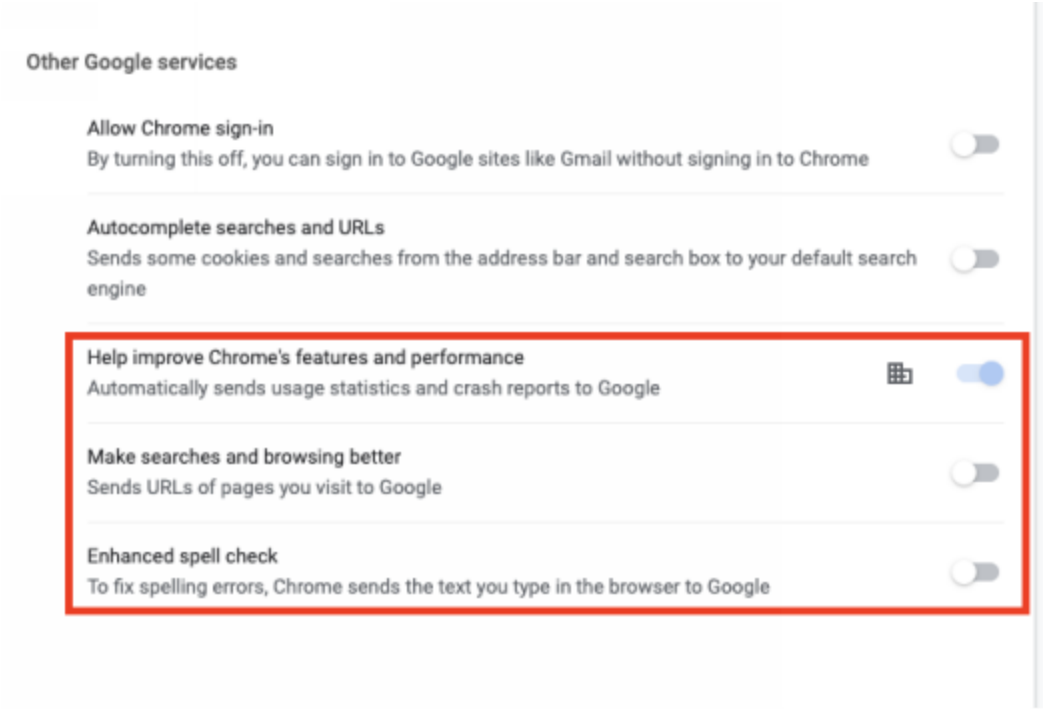


## Festlegen, wer die Chrome-Synchronisierung verwenden darf, und Tipps zu anderen Chrome-Einstellungen geben

Mit der Chrome-Synchronisierung können Nutzer Lesezeichen, Verlauf, Passwörter und weitere Einstellungen sicher in ihren von der Organisation verwalteten Google-Konten speichern und über Chrome von jedem Gerät aus darauf zugreifen. Als Administrator können Sie die Chrome-Synchronisierung für von der Organisation verwaltete Nutzerkonten aktivieren oder deaktivieren. Gehen Sie dazu in der Admin-Konsole zu *Zusätzliche Google-Dienste > Google Chrome-Synchronisierung*. Wenn die Chrome-Synchronisierung aktiviert ist, können die Nutzer synchronisierte Informationen auf jedem Gerät sehen und aktualisieren, wie beispielsweise Lesezeichen, Verlauf, Passwörter und andere Einstellungen.

Außerdem haben sie die Möglichkeit, auszuwählen, welche Google-Funktionen sie in Chrome verwenden möchten, beispielsweise:

- **Helfen, die Funktionen und die Leistung von Chrome zu verbessern**: Die Übertragung von Absturzberichten und Nutzungsstatistiken an Google ist standardmäßig aktiviert, kann aber vom Nutzer in den Chrome-Einstellungen deaktiviert werden. Nutzungsstatistiken enthalten z. B. Informationen zu Einstellungen, zu Klicks auf Schaltflächen oder zur Speicherauslastung. Im Allgemeinen enthalten die Nutzungsstatistiken von Chrome keine Webseiten-URLs oder personenbezogenen Daten. Wenn der Nutzer in den Chrome-Einstellungen jedoch die Option *Suchanfragen und das Surfen verbessern* aktiviert hat, enthält die Chrome-Nutzungsstatistik auch Informationen darüber, welche Webseiten der Nutzer besucht und wie er sie verwendet hat. Wenn die Chrome-Synchronisierung aktiviert ist, können außerdem Angaben zu Alter und Geschlecht aus dem von der Organisation verwalteten Google-Konto des Nutzers mit unseren Statistiken kombiniert werden. Mithilfe dieser demografischen Merkmale lassen sich unsere Produkte weiter verbessern. Diese Informationen werden nur in zusammengefasster Form verwendet und lassen keinen Rückschluss auf den Nutzer zu. Absturzberichte enthalten Systeminformationen zum Zeitpunkt des Absturzes. Je nachdem, was beim Absturz passiert ist, werden darin auch URLs von Webseiten oder personenbezogene Daten berücksichtigt. Raten Sie den Nutzern, diese Einstellung entsprechend ihren persönlichen Anforderungen und den Unternehmensrichtlinien zu deaktivieren oder zu aktivieren. Eine Anleitung dazu finden Sie im Hilfeartikel Automatisch gesendete Berichte zu Fehlern und Abstürzen ein- oder ausschalten.




- **Erweiterte Rechtschreibprüfung**: Bei der einfachen Rechtschreibprüfung wird ein lokales Wörterbuch verwendet. Bei der cloudbasierten erweiterten Rechtschreibprüfung dagegen wird der eingegebene Text an Google gesendet. Standardmäßig ist für Ihre Nutzer die einfache Rechtschreibprüfung aktiviert. Die Nutzer können jedoch in den Chrome-Einstellungen unter *Google und ich > Erweitert > Sprachen* die erweiterte Rechtschreibprüfung auswählen. Wenn die erweiterte Rechtschreibprüfung aktiviert ist, wird der gesamte Inhalt der Textfelder während der Eingabe zusammen mit der Standardsprache des Browsers an Google gesendet. Die erweiterte Rechtschreibprüfung gehört nicht zu den Google Workspace-Hauptdiensten und unterliegt deshalb weder den Google Workspace-Vereinbarungen noch dem Zusatz zur Datenverarbeitung. Die über die erweiterte Rechtschreibprüfung an Google gesendeten Daten werden gemäß der Datenschutzerklärung und den Nutzungsbedingungen von Google sowie den zusätzlichen Nutzungsbedingungen für Google Chrome und Chrome OS verarbeitet.

Wenn Ihre Organisation eine strengere Kontrolle über die Chrome-Einstellungen durch den Administrator benötigt und festlegen muss, welche Daten mit Google und Dritten über Chrome geteilt werden dürfen, ist Chrome Enterprise vielleicht das Richtige für Sie. Dieser Dienst bietet Administratoren verschiedene Optionen zum Festlegen von Datenschutzrichtlinien für ihre Organisation. Beispielsweise können Administratoren die Richtlinie Berichterstellung für Messwerte für alle Nutzer der Organisation so einstellen, dass keine Absturzdaten und anonymen Nutzungsberichte an Google gesendet werden. Administratoren haben außerdem die Möglichkeit, die erweiterte Rechtschreibprüfung für ihre Organisation zu deaktivieren oder zu aktivieren. Weitere Informationen finden Sie im Leitfaden für die Chrome-Verwaltung über die Cloud und im Konfigurationshandbuch für die Sicherheitseinstellungen von Google Chrome für Unternehmen.

## Nutzern innerhalb der Domain unterschiedliche Zugriffsrechte erteilen

Als Administrator können Sie den Nutzerzugriff auf verschiedene Google Workspace-Dienste und zusätzliche Produkte verwalten, indem Sie Organisationseinheiten erstellen. So lassen sich die Nutzer in verschiedene Gruppen einteilen, beispielsweise in eine Gruppe von Nutzern, die personenbezogene und sensible Daten verwalten darf, und eine andere Gruppe, auf die das nicht zutrifft. Sobald diese Organisationseinheiten eingerichtet sind, können Sie bestimmte Dienste und Produkte für die jeweilige Nutzergruppe aktivieren oder deaktivieren.

Ein Beispiel: Die Personalabteilung verwaltet personenbezogene und sensible Daten, aber nicht alle Nutzer in dieser Abteilung müssen auf diese Daten zugreifen. In diesem Fall können Sie eine Organisationseinheit „Personalabteilung“ für Nutzer erstellen, die die Google Workspace-Hauptdienste mit personenbezogenen und sensiblen Daten verwenden, und für diese Gruppe bestimmte Dienste deaktivieren sowie Einstellungen entsprechend konfigurieren.

## Nutzern die Trennung zwischen von der Organisation verwalteten Google-Konten und privaten Konten empfehlen

Nutzer sollten den Zugriff auf ihr von der Organisation verwaltetes Google-Konto und den Zugriff auf ihr privates Google-Konto trennen. Raten Sie Ihren Nutzern, sich nicht gleichzeitig im selben Chrome-Browser in mehreren Google-Konten anzumelden. Dadurch ist das Risiko verringert, dass beispielsweise versehentlich Kundendaten im privaten Konto eines Nutzers gespeichert oder die Datenschutzeinstellungen eines privaten Google-Kontos auf ein von der Organisation verwaltetes Google-Konto angewendet werden.

Wenn Ihre Organisation eine strengere Kontrolle benötigt, können Sie festlegen, dass sich Nutzer in Google-Diensten nicht mit anderen Konten als den von Ihnen eingerichteten Konten anmelden dürfen, etwa mit privaten Gmail-Konten oder einem von der Organisation verwalteten Google-Konto aus einer anderen Domain. Eine Anleitung finden Sie im Hilfeartikel Zugriff auf Privatnutzerkonten blockieren.[7]

Als Administrator können Sie außerdem die geschäftlichen Apps und Daten auf Android-Geräten sicher verwalten, während Sie den Nutzern die Kontrolle über private Apps und Daten überlassen. Mit Arbeitsprofilen[8] auf Android-Geräten lassen sich geschäftliche Apps und Daten von privaten Apps und Daten trennen. In diesem Hilfeartikel erfahren Sie mehr darüber, wie Sie ein Arbeitsprofil einrichten und bevorzugte geschäftliche Apps auf eine Zulassungsliste setzen.

## Empfehlungen zum Sicherheitsstatus prüfen

Wenn Sie regelmäßig die Empfehlungen auf der Seite Sicherheitsstatus in der Admin-Konsole lesen, können Sie die Daten Ihrer Organisation besser schützen. Sehr hilfreich ist auch die Sicherheits-Checkliste für mittlere und große Unternehmen in der Google Workspace-Admin-Hilfe.

Administratoren stehen außerdem viele leistungsstarke Sicherheitstools zur Verfügung und sie können ihre individuellen Sicherheitseinstellungen an die geschäftlichen Anforderungen anpassen. In der Benachrichtigungszentrale für Google Workspace finden Sie beispielsweise Benachrichtigungen und umsetzbare Sicherheitswarnungen zu Aktivitäten in Ihrer Domain, mit denen Sie die Organisation besser vor den neuesten Sicherheitsbedrohungen schützen können, wie beispielsweise Phishing oder verdächtige Geräteaktivitäten. Und mit dem Sicherheits-Prüftool lassen sich Sicherheits- und Datenschutzprobleme in Ihrer Domain erkennen und sichten und Sie können entsprechende Maßnahmen ergreifen. Administratoren haben außerdem die Möglichkeit, im Prüftool Aktivitätsregeln festzulegen, nach denen bestimmte Aktionen automatisch ausgeführt werden. So können Sie Sicherheitsprobleme noch schneller und effizienter erkennen und beheben. Darüber hinaus lassen sich mit Google Vault Daten verwalten, aufbewahren und exportieren, um die Anforderungen Ihrer Organisation an Aufbewahrung und E-Discovery zu erfüllen. Diese und viele weitere Sicherheitstools sind auf der Seite Sicherheit und Vertrauen in Google Workspace beschrieben.

## Nutzung von Drittanbieter-Apps in Ihrer Organisation prüfen

In einigen Google Workspace-Hauptdiensten können Nutzer je nach Einstellungen für die Domain personenbezogene Kundendaten für Dritte (oder eine Drittanbieter-App) freigeben. Kunden sind daher dafür verantwortlich, angemessene Maßnahmen für diese Freigabe an Dritte (oder Drittanbieter-Apps) zu ergreifen, bevor personenbezogene Kundendaten freigegeben oder übertragen werden. Ihre Organisation muss vor der Freigabe personenbezogener und sensibler Daten an Dritte über Google Workspace-Dienste oder damit verknüpfte Apps feststellen, ob dafür gesonderte Datenschutzbedingungen erforderlich sind.

Als Administrator haben Sie drei Möglichkeitenzur Verwaltung des Google Workspace Marketplace. Sie können die Installation aller Apps verbieten, nur die Installation von Apps auf der Zulassungsliste erlauben oder die Installation aller Apps erlauben. Standardmäßig ist Google Workspace-Nutzern die Installation aller verfügbaren Apps vom Google Workspace Marketplace erlaubt. Sie sollten sich die Unternehmensrichtlinien ansehen und nur ausgewählte Drittanbieter-Apps auf die Zulassungsliste setzen, die auf API-Bereiche in den Google Workspace-Diensten zugreifen dürfen.

Über die App-Zugriffssteuerung können Sie außerdem festlegen, welche Apps von Drittanbietern und Domaininhabern auf vertrauliche Google Workspace-Daten zugreifen dürfen. Die Zugriffssteuerung bietet folgende Möglichkeiten:

- Den Zugriff auf die meisten Google Workspace-Dienste einschränken oder uneingeschränkt lassen
- Bestimmte Apps als vertrauenswürdig einstufen, damit sie auf eingeschränkte Google Workspace-Dienste zugreifen können
- Alle domaininternen Apps als vertrauenswürdig einstufen

Der Zugriff auf Kundendaten ist für alle installierten Marketplace-Apps standardmäßig aktiviert. Wir empfehlen Ihnen, den Zugriff auf Ihre Google Workspace-Kundendaten gemäß den Unternehmensrichtlinien bei Bedarf einzuschränken.

## Kontoaktivität im Blick behalten

Die Berichte und Audit-Logs der Admin-Konsole bieten viele Möglichkeiten. So können Sie beispielsweise ganz einfach mögliche Sicherheitsrisiken analysieren, die Zusammenarbeit von Nutzern messen, Anmeldeaktivitäten erfassen und Administratoraktivitäten analysieren. Administratoren können sich benachrichtigen lassen, wenn Google bestimmte Aktivitäten erkennt – beispielsweise verdächtige Anmeldeaktivitäten, gesperrte Nutzer, hinzugefügte Nutzer, gesperrte und wieder aktivierte Nutzer, gelöschte Nutzer, von einem Administrator vorgenommene Passwortänderungen, Nutzer mit neuen Administratorberechtigungen und Nutzer mit aufgehobenen Administratorberechtigungen. Administratoren sollten sich Berichte und Audit-Logs regelmäßig ansehen, um mögliche Sicherheitsrisiken zu untersuchen. Hier finden Sie wichtige Trends im Bereich Highlights, das Risiko von Datenschutzverletzungen unter Sicherheit, die in Apps erstellten Dateien unter Nutzeraktivität sowie den Bereich Kontoaktivität und Audits mit hilfreichen Informationen zu Sicherheitsrisiken.

Während die Audit-Logs für Administratoren Informationen zu Aktionen von Mitgliedern in ihrer eigenen Organisation enthalten, bietet Access Transparency[9] Logs zu Aktionen, die von Google-Mitarbeitern ausgeführt wurden. Die Access Transparency-Logs enthalten Informationen über die Ressource, auf die zugegriffen wurde, sowie zur Aktion und zum Zeitpunkt und Grund der Aktion (beispielsweise die zu einer Kundensupport-Anfrage gehörende Bearbeitungsnummer).

## Datenschutzrichtlinien für Dateinamen und Pfadnamen festlegen

Als zusätzliche Sicherheitsvorkehrung, um die Freigabe personenbezogener Kundendaten einzuschränken, können Sie Richtlinien festlegen, mit denen Sie verhindern, dass Nutzer beim Benennen und Organisieren von Dateien in den Google Workspace-Hauptdiensten (beispielsweise Google Docs, Google Tabellen, Google Präsentationen, Google Formulare, Google Drive und Gmail) oder in den Namen von Chatrooms in Google Chat oder in Google Meet-Einladungen vertrauliche Informationen oder personenbezogene Daten verwenden. Zu personenbezogenen Kundendaten zählen unter anderem der vollständige Name einer Person sowie ihre E-Mail-Adresse, Postanschrift, Telefonnummer oder eine eindeutige Kontokennung (beispielsweise Kunden-ID, Projekt-ID und Bildschirmname).

Außerdem können Sie die Optionen zum Schutz vor Datenverlust (Data Loss Prevention, DLP) in Google Workspace verwenden, um sensible Daten zu prüfen, zu klassifizieren und zu de-identifizieren und so Risiken zu minimieren. Weitere Informationen finden Sie in den Hilfeartikeln Neue DLP-Version für Google Drive und E-Mail-Verkehr mit der Funktion „Schutz vor Datenverlust“ überprüfen. Wir stellen Ihnen vordefinierte Inhaltsdetektoren zur Verfügung, um die Einrichtung zu vereinfachen. Sobald die DLP-Richtlinien festgelegt wurden, kann Gmail beispielsweise automatisch alle ausgehenden E-Mails auf vertrauliche Informationen prüfen. Außerdem lassen sich Maßnahmen gegen Datenlecks einleiten: E-Mails zur Überprüfung unter Quarantäne stellen, ausgehende E-Mails blockieren und die Sender

benachrichtigen oder Nutzer zum Ändern der Informationen auffordern. DLP für Google Drive umfasst leicht konfigurierbare Regeln und eine optische Zeichenerkennung für Text in Bildern. So können Administratoren Dateien mit vertraulichen Inhalten ganz einfach prüfen und Regeln konfigurieren, um Nutzer vor der externen Freigabe vertraulicher Daten zu warnen und diese zu verhindern. Weitere Informationen finden Sie in unserem Whitepaper zum Schutz vor Datenverlust.

# Zusätzliche Ressourcen

Wir möchten unsere Kunden bei Compliance und Berichterstellung unterstützen. Deshalb bieten wir Anleitungen und Best Practices zum Datenschutz und einfachen Zugriff auf Dokumente. Unsere Produkte werden regelmäßig von unabhängigen Dritten auf Sicherheit, Datenschutz und Compliance überprüft und sind nach weltweit anerkannten Standards zertifiziert. Eine Liste aller Standards, Regelungen und Zertifizierungen von Google Workspace finden Sie in unserem Center für Compliance-Ressourcen.

Informationen zu einem einfachen On-Demand-Zugriff auf diese wichtigen Ressourcen ohne Zusatzkosten finden Sie in unserer Übersicht über Complianceberichte. Zu den wichtigsten Ressourcen gehören unsere neuesten ISO/IEC-Zertifizierungen, SOC-Berichte und Selbsteinschätzungen. Für einige Ressourcen ist möglicherweise eine Anmeldung über Ihre Google Cloud-Plattform oder Ihr Google Workspace-Konto erforderlich.

Weitere Informationen dazu, wie die Google Workspace-Dienste unter Berücksichtigung von Datenschutz, Vertraulichkeit, Integrität und Verfügbarkeit von Daten konzipiert wurden, finden Sie hier:

- **Google Cloud-Datenschutz**: Eine Auflistung der Google Cloud-Vertrauensgrundsätze
- **Sicherheit und Vertrauen in Google Workspace**: Webseite zum Thema Sicherheit bei Google Cloud mit Links zu Whitepapers und weiteren Ressourcen zu Datenschutz, Transparenz, Infrastruktur und Sicherheitsprodukten
- **Google Workspace-Admin-Hilfe**: Website mit Links zu Anleitungen und technischen Dokumenten für Google Workspace-Produkte und Sicherheitsfunktionen
- **Center für DSGVO-Ressourcen**: Zusammenstellung der erforderlichen Informationen zu Vorschriften, Compliance und Produkten zur Einhaltung der DSGVO
- **Vertrauen und Sicherheit**: Whitepapers, Videos, Artikel, Blogposts und Dokumente zu Datenschutz und Sicherheit

# Anhang 1: Zuordnung von Datenschutzeinstellungen

Mit dieser Zuordnung von Datenschutzeinstellungen lässt sich ganz einfach einschätzen, was Sie bei der Verwendung von Google Workspace brauchen, um die Anforderungen verschiedener Datenschutzvorschriften zu erfüllen. Hierbei handelt es sich nicht um eine vollständige Liste aller Datenschutzeinstellungen, sondern nur um eine allgemeine Zuordnung. Sie sollten einen Rechtsexperten hinzuziehen, um sich zu den besonderen Anforderungen beraten zu lassen, die für Ihre Organisation gelten, denn dieser Leitfaden ist nicht als Rechtsberatung zu verstehen.

## Aufgaben als Datenverantwortlicher

| Typische Datenschutzeinstellungen | Verantwortung des Kunden | Unterstützende Google Workspace-Funktionen |
|---|---|---|
| **Kenntnis der Organisation und ihres Kontexts** | Die Organisation muss ihre Rolle als Verantwortlicher für personenidentifizierbare Informationen und/oder als Auftragsverarbeiter solcher Informationen definieren, um die entsprechenden (behördlichen usw.) Anforderungen für die Verarbeitung personenbezogener Kundendaten ermitteln zu können. | Weitere Informationen zu Rollen und Berechtigungen bei der Verarbeitung von Kundendaten finden Sie in Paragraf 5 im Zusatz zur Datenverarbeitung für Google Workspace. |
| **Festlegen, wann Einwilligungen einzuholen sind, und Einwilligungen speichern** | Der Kunde muss die rechtlichen oder behördlichen Anforderungen für den Erhalt von Einwilligungen von Einzelpersonen vor der Verarbeitung personenbezogener Kundendaten kennen und die Einwilligung bei Bedarf speichern. | Google bietet keine Unterstützung für den Erhalt und die Speicherung von Nutzereinwilligungen für alle Ihre Aktivitäten.<br><br>Wenn sich Nutzer in dem von der Organisation verwalteten Google-Konto anmelden, das für sie erstellt wurde, erhalten sie eine Mitteilung dazu, wie der Administrator ihre Daten erhebt und darauf zugreift. |
| **Rechtmäßigkeit der Verarbeitung und Zweck des Dokuments ermitteln** | Der Kunde sollte sich mit allen Anforderungen in Bezug auf die Rechtmäßigkeit der Verarbeitung vertraut machen, z. B. eine gegebenenfalls erforderliche Einwilligung. Der Kunde muss den Zweck dokumentieren, für den | Google bietet für alle Ihre Aktivitäten keinen Support bei der Ermittlung der Rechtmäßigkeit der Verarbeitung.<br><br>Weitere Informationen zur Verarbeitung seitens Google und zum Zweck dieser Verarbeitung finden Sie in den Nutzungsbedingungen für |

| | | |
|---|---|---|
| | personenbezogene Kundendaten verarbeitet werden. | Google Workspace und imZusatz zur Datenverarbeitung. |
| **Verträge mit Auftragsverarbeitern personenidentifizierbarer Informationen** | Der Kunde sollte sicherstellen, dass seine Verträge mit Auftragsverarbeitern Anforderungen zur Hilfestellung in Bezug auf alle relevanten rechtlichen oder gesetzlichen Verpflichtungen enthalten, die sich auf die Verarbeitung und den Schutz personenbezogener Kundendaten beziehen. | In seiner Rolle als Datenauftragsverarbeiter unterstützt Google Sie bei der Einhaltung Ihrer Verpflichtungen (unter Berücksichtigung der Art der Verarbeitung personenbezogener Kundendaten und der Google zur Verfügung stehenden Informationen) in Übereinstimmung mit demZusatz zur Datenverarbeitung. Weitere Informationen finden Sie in den Abschnitten 7.1.4 (Sicherheitsunterstützung), 9.2.2 (Unterstützung bei Anfragen von betroffenen Personen) und 8.1 (DSFA-Unterstützung). |
| **Erhebung und Verarbeitung beschränken** | Der Kunde muss die Anforderungen in Bezug auf Beschränkungen für die Erhebung und Verarbeitung personenbezogener Kundendaten kennen, z. B., dass Erhebung und Verarbeitung auf die für den genannten Zweck erforderlichen Informationen beschränkt werden müssen. | Weitere Informationen zur Verarbeitung seitens Google und zum Zweck dieser Verarbeitung finden Sie in den Nutzungsbedingungen für Google Workspace und imZusatz zur Datenverarbeitung. |
| **Datensätze in Bezug auf die Verarbeitung personenidentifizierbarer Informationen** | Der Kunde muss alle notwendigen und geforderten Datensätze in Bezug auf die Verarbeitung personenbezogener Daten aufbewahren. | Google Workspace bietet Audit-Logs, um den Datenzugriff sichtbar zu machen und Ihnen bei der Beantwortung folgender Fragen zu helfen: *Wer hat was getan? Wo und wann wurde es getan?* Zu den verfügbaren Audit-Logs zählen Aktivitätsprotokolle (Admin-Audit-Log), Sicherheitsprotokolle (Anmeldung, SAML und Access Transparency) sowie Nutzerdienste und Kontoprotokolle (E-Mail-Protokollsuche und Drive-Audit-Log). Im Hilfeartikel Verfügbare Audit-Logs erfahren Sie mehr darüber. Im Allgemeinen müssen Audit-Logs sechs Monate aufbewahrt werden. Weitere Informationen finden Sie unter Datenaufbewahrung und Zeitverzögerungen. Sie können anpassen, wasin einem Audit-Log in der Google-Admin-Konsole angezeigt wird, indem Sie nach Nutzer oder Aktivität, Organisationseinheit oder Datum filtern. Außerdem lassen sich für bestimmte Aktivitäten Benachrichtigungen einrichten. |

## Organisatorische Datenschutzrichtlinien und -prüfung

| Typische Datenschutzeinstellungen | Verantwortung des Kunden | Unterstützende Google Workspace-Funktionen |
|---|---|---|
| **Unabhängige Prüfung der Informationssicherheit** | Der Kunden muss ein Verfahren zur Risikobeurteilung für Informationssicherheit anwenden, um Risiken in Zusammenhang mit dem Verlust von Vertraulichkeit, Integrität und Verfügung zu ermitteln. Dies kann interne oder externe Audits oder andere Maßnahmen zur Beurteilung der Verarbeitungssicherheit umfassen. Wenn der Kunden die Verarbeitung ganz oder teilweise von einer anderen Organisation oder einem Drittanbieter durchführen lässt, sollten Informationen zu diesen Beurteilungen erfasst werden. | Sie sind für Ihre Nutzung der Dienste und die Speicherung von Kopien Ihrer Kundendaten außerhalb der Google-Systeme oder der Systeme von Google-Unterauftragsverarbeitern verantwortlich.<br><br>Google unterzieht sich regelmäßig einer steigenden Zahl von Prüfungen durch verschiedene unabhängige Dritte. Bei den Kontrollen analysieren unabhängige Prüfer unsere Rechenzentren, unsere Infrastruktur und unseren laufenden Betrieb eingehend. Es werden regelmäßige Prüfungen durchgeführt, um unsere Einhaltung der Prüfungsstandards ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 und SOC 2 zu zertifizieren. Eine Liste der Compliance-Zertifizierungen finden Sie im Center für Compliance-Ressourcen von Google Cloud.<br><br>Auf der Basis Ihrer Vertragsbedingungen mit Google als Google Workspace-Kunde kann Google Ihnen – oder einem von Ihnen ernannten unabhängigen Prüfer – in Übereinstimmung mit Abschnitt 7.5 (Prüfungen und Compliance-Audits) im Zusatz zur Datenverarbeitung die Durchführung von Prüfungen (einschließlich Inspektionen) gestatten, um zu bestätigen, dass Google seinen Pflichten nachkommt. |
| **Datenschutz-Folgenabschätzung (DSFA)** | Der Kunde muss die Anforderungen für die Durchführung einer Datenschutz-Folgenabschätzung kennen (Zeitpunkt der Durchführung, was muss die Abschätzung enthalten, wer führt | Als Datenauftragsverarbeiter unterstützt Google Sie bei der Einhaltung Ihrer Verpflichtungen in Bezug auf die Datenschutz-Folgenabschätzung (unter Berücksichtigung der Art der Verarbeitung und der Google zur Verfügung stehenden Informationen) in |

| | | |
|---|---|---|
| | sie durch usw.). | Übereinstimmung mit Abschnitt 8 im Zusatz zur Datenverarbeitung. |
| **Geltungsbereich des Managementsystems für Informationssicherheit festlegen** | Ein Gesamtprogramm für Sicherheit oder Datenschutz, das ein Kunde möglicherweise hat, sollte die Verarbeitung personenbezogener Kundendaten und die diesbezüglichen Anforderungen abdecken.<br><br>Richtlinien für Systementwicklung und -aufbau sollten eine Anleitung zur Verarbeitung personenidentifizierbarer Informationen durch die Organisation umfassen, basierend auf Verpflichtungen gegenüber den betroffenen Personen und/oder geltenden Gesetzen und/oder Vorschriften und der jeweiligen Art der von der Organisation durchgeführten Verarbeitung. | Google bietet keine Unterstützung für das interne Verfahren seiner Kunden.<br><br>Sie sollten mindestens jährlich die Erstellung von Datenschutzrichtlinien und zugehörigen Schulungsmaterialien erwägen, die an Nutzer und an mit dem Datenschutz betraute Mitarbeiter in Ihrer gesamten Organisation ausgegeben werden. Google bietet Professional Services für die Unterweisung der Nutzer in Cloud-Sicherheit und -Datenschutz an, darunter unter anderem eine Google Workspace-Sicherheitsbeurteilung. |
| **Richtlinien zur Informationssicherheit** | Der Kunde sollte seine Richtlinien zur Informationssicherheit um den Schutz personenbezogener Kundendaten erweitern, einschließlich Richtlinien, die zur Einhaltung geltender Gesetze erforderlich sind. Der Kunde sollte Verantwortlichkeiten für relevante Schulungen in Bezug auf den Schutz personenbezogener Kundendaten festlegen und zuweisen. | Google bietet keine direkte Unterstützung für das interne Verfahren seiner Kunden.<br><br>Erwägen Sie eine organisationsweite Sicherheits- und Datenschutzbeurteilung und Autorisierungsrichtlinie, in der die Verfahren und Anforderungen an die Umsetzung von Datenschutzbeurteilungen, Datenschutzeinstellungen und Autorisierungskontrollen des Unternehmens definiert werden. |
| **Organisation der Informationssicherheit für Kunden** | Der Kunde sollte innerhalb seiner Organisation Verantwortlichkeiten in Bezug auf die Sicherheit und den Schutz personenbezogener Kundendaten definieren. Dies kann auch die Einrichtung bestimmter Rollen für Datenschutzbelange umfassen, einschließlich eines Datenschutzbeauftragten (DSB). Hierbei sollten geeignete | Google bietet keine direkte Unterstützung für das interne Verfahren seiner Kunden.<br><br>Erwägen Sie die Ernennung einer oder mehrere Personen, die für die Entwicklung, Umsetzung, Verwaltung und Überwachung eines organisationsweiten Governance- und Datenschutzprogramms zuständig sind, um die Einhaltung aller geltenden Gesetze und Vorschriften in |

| | | |
|---|---|---|
| | Schulungen und Unterstützung bei der Verwaltung eingeplant werden. | Bezug auf die Verarbeitung personenidentifizierbarer Informationen sicherzustellen.<br><br>Sie können Ihren Datenschutzbeauftragten und EU-Vertreter in der Google-Admin-Konsole unter **Kontoeinstellungen > Recht und Compliance** benennen.<br><br>Google hat einen Datenschutzbeauftragten für Google LLC und seine Tochtergesellschaften für die Bereiche der Datenverarbeitung ernannt, die verschiedenen Datenschutzgesetzen unterliegen. |
| **Klassifizierung von Informationen** | Der Kunde sollte die Verwendung personenidentifizierbarer Informationen explizit als Teil eines Schemas zur Datenklassifizierung ansehen. | Google bietet keine Unterstützung für das interne Verfahren seiner Kunden.<br><br>Ihr System zur Datenklassifizierung sollte die Verwendung personenidentifizierbarer Informationen explizit als Teil des von Ihnen angewendeten Schemas umfassen. Die Berücksichtigung personenidentifizierbarer Informationen im Gesamtklassifizierungssystem ist unabdingbar, um zu verstehen, welche Art oder Sonderkategorie an personenidentifizierbaren Informationen Sie verarbeiten, wo diese Informationen gespeichert sind und durch welche Systeme sie geleitet werden können.<br><br>Ihr Datenklassifizierungsschema sollte beschreiben, wie Sie Daten in Abhängigkeit von ihrer Vertraulichkeit und Identifizierbarkeit klassifizieren. Dateneigentümer sind dafür verantwortlich, die jeweilige Datenklassifizierung auf folgender Basis festzulegen: Wer benötigt Zugriff und für welchen Zweck, welche potenziellen Risiken und Schäden gibt es bei unbefugtem Zugriff auf die Daten und was ist der allgemeine Kontext der Daten. |

| | | |
|---|---|---|
| **Umgang mit Informationssicherheitsvorfällen** | Der Kunde sollte Verfahren einsetzen, mit denen ermittelt werden kann, wann eine Verletzung des Schutzes personenbezogener Kundendaten vorliegt.<br><br>Der Kunde sollte wissen, wofür er bei einer Datenpanne oder einem Sicherheitsvorfall in Bezug auf personenbezogene Kundendaten verantwortlich ist, und dies entsprechend dokumentieren. Beispiele für Verantwortlichkeiten sind unter anderem die Benachrichtigung der jeweiligen Parteien, die Kommunikation mit Auftragsverarbeitern oder anderen Drittunternehmen und Verantwortlichkeiten innerhalb der Organisation des Kunden. | Sie sollten für Ihre Organisation eine Richtlinie zur Reaktion auf Vorfälle einführen, die Verfahren zur Bereitstellung und Umsetzung von Steuerungen der Reaktionen auf Vorfälle enthält, und Sie sollten Sicherheitsgruppen für Behörden und für die Teams Ihrer Organisation erstellen, die mit der Reaktion auf Vorfälle betraut sind.<br><br>Außerdem ist es empfehlenswert, einen Testplan für die Reaktionen auf Vorfälle, Verfahren, Checklisten, Anforderungen und Maßstäbe in Bezug auf den Erfolg zu entwickeln. Erwägen Sie, Vorfallsklassen zu definieren, die von Ihrer Organisation erkannt werden, und legen Sie die als Reaktion auf diese Vorfälle jeweils zu ergreifenden Maßnahmen fest. Erwägen Sie auch die Definition bestimmter Maßnahmen, die von autorisierten Mitarbeitern im Falle eines Vorfalls zu ergreifen sind, wie beispielsweise Schritte für das Management versehentlich offengelegter personenidentifizierbarer Informationen sowie von Cybersicherheit-Schwachstellen und -Angriffen.<br><br>Nutzen Sie außerdem die Funktionen in Google Workspace umE-Mail-Inhalte zu scannen und zu isolieren,Phishing-Versuche zu blockieren undBeschränkungen für Anhänge einzurichten. Mithilfe des Schutzes vor Datenverlust (DLP) können Sie sensible Daten prüfen, klassifizieren und de-identifizieren, um die Offenlegung einzuschränken. Weitere Informationen: Schutz vor Datenverlust mit dem neuen DLP für Google Drive, E-Mail-Verkehr mit der Funktion „Schutz vor Datenverlust“ überprüfen, Whitepaper zum Schutz vor Datenverlust |

| | | |
|---|---|---|
| | | Als Google-Kunde werden Sie von Google sofort benachrichtigt, sobald ein Datenvorfall bekannt wird, und es werden umgehend geeignete Schritte zur Schadensbegrenzung und zum Schutz von Kundendaten unternommen. Weitere Informationen zu unserer Selbstverpflichtung finden Sie in Abschnitt 7.2 (Datenvorfall) im Zusatz zur Datenverarbeitung . Hier erfahren Sie, wie wir auf Datenvorfälle reagieren. |
| **Informationssicherung** | Der Kunde sollte eine Richtlinie haben, in der die Anforderungen für Datensicherheit und die Wiederherstellung personenidentifizierbarer Informationen (auch als Teil einer allgemeinen Richtlinie zur Informationssicherheit) und jegliche weiteren Anforderungen (z. B. vertragliche und/oder rechtliche) für das Löschen personenidentifizierbarer Informationen festgelegt werden, die in für Sicherungszwecke gespeicherten Daten enthalten sind. | Sie sollten einen Notfallplan für Ihre Organisation entwickeln, der die Verfahren und die Umsetzungsanforderungen für die Steuerung von Notfallplänen in Ihrer Organisation festlegt.<br>Darüber hinaus sollten Sie die wichtigsten Mitarbeiter, Rollen und Zuständigkeiten im Notfall für alle organisatorischen Elemente angeben.<br><br>Heben Sie außerdem die für die Zielsetzung und das Unternehmen wesentlichen Vorgänge des Informationssystems in Ihrer Organisation hervor. Legen Sie Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) für die Wiederaufnahme der wesentlichen Vorgänge nach der Aktivierung des Notfallplans fest.<br><br>Dokumentieren Sie wichtige Informationssysteme und zugehörige Software. Ermitteln Sie zusätzliche sicherheitsbezogene Informationen und legen Sie Leitlinien und Anforderungen für die Speicherung von Sicherungskopien wichtiger Systemkomponenten und -daten fest.<br><br>Google besitzt und betreibtRechenzentren auf der ganzen Welt, die dazu beitragen, dass das Internet rund um die Uhr funktioniert, und |

| | | |
|---|---|---|
| | | unseren Kunden Redundanz und Resilienz bieten. Sie können auch zusätzliche Sicherungen ausführen und Ihre lokalen Daten mit Google Drive synchronisieren. |

## Datenschutz- und Sicherheitseinstellungen

| Typische Datenschutzeinstellungen | Verantwortung des Kunden | Unterstützende Google Workspace-Funktionen |
|---|---|---|
| **Verwaltung des Nutzerzugriffs (einschließlich Einrichtung des Nutzerzugriffs und Verwaltung privilegierter Zugriffsrechte)** | Der Kunden sollte wissen, welche Verantwortungen er für die Zugriffssteuerung bei dem von ihm genutzten Dienst hat, und diese Verantwortungen mithilfe der verfügbaren Tools entsprechend verwalten. | Sie sollten eine organisationsweite Richtlinie für die Zugriffssteuerung für Informationssysteme in der Cloud entwickeln. Sie sollten außerdem die Parameter und Verfahren definieren, mit denen Ihre Organisation Informationen erstellt, aktiviert, ändert und deaktiviert sowie aus Systemkonten entfernt.<br><br>Die Google-Admin-Konsole bietet Ihnen eine zentralisierte Verwaltung, sodass Einrichtung und Verwaltung effizienter werden. Sie können Ihre Organisation mit Sicherheitsanalysen und Best Practices-Empfehlungen im Sicherheitscenter schützen. Sie können mithilfe von Cloud Identity and Access Management (IAM) administrativen Gruppen Rollen und Berechtigungen zuweisen und dabei das Prinzip der geringsten Berechtigung und Aufgabentrennung heranziehen. Hier erfahren Sie, wie Sie Ihrem Google Workspace-Konto Cloud Identity hinzufügen. |
| **Sichere Anmeldeverfahren** | Der Kunde sollte für alle Nutzerkonten, die seiner Kontrolle unterliegen, Mechanismen für eine sichere Anmeldung einrichten. | Als Google Workspace-Kunde können Sie integrierte Cloud Identity-Funktionen zur Verwaltung von Nutzern verwenden und Sicherheitsoptionen wie beispielsweise die Bestätigung in zwei Schritten und Sicherheitsschlüssel einrichten.<br><br>Mit der Bestätigung in zwei Schritten |

| | | |
|---|---|---|
| | | fügen Sie den Google Workspace-Konten eine zusätzliche Sicherheitsebene hinzu, indem Sie die Nutzer auffordern, bei der Anmeldung nicht nur ihren Benutzernamen und das Passwort, sondern auch einen Bestätigungscode einzugeben.<br><br>Der Sicherheitsschlüssel ist eine Erweiterung der Bestätigung in zwei Schritten. Google hat den Sicherheitsschlüssel in Zusammenarbeit mit der Standardisierungsorganisation FIDO Alliance entwickelt: Dies ist ein physischer Schlüssel für den Zugriff auf Ihr von der Organisation verwaltetes Google-Konto. Er sendet eine kryptografische Signatur und keinen Code. Dadurch wird sichergestellt, dass Ihre Anmeldedaten nicht durch Phishing abgegriffen werden können. Weitere Informationen finden Sie unter Sicherheitsschlüssel für die Bestätigung in zwei Schritten.<br><br>Weitere Informationen zur Nutzerauthentifizierung und zu Autorisierungsfunktionen finden Sie im Google Cloud-Whitepaper zu Sicherheit und Compliance. |

| | | |
|---|---|---|
| **Ereignisprotokollierung und Schutz** | Der Kunde sollte mit den Funktionen für die Protokollierung vertraut sein, die vom System bereitgestellt werden. Er sollte mit diesen Funktionen sicherstellen, dass Aktionen, für die dies erforderlich ist, für personenbezogene Kundendaten protokolliert werden können.<br><br>Es sollte ein Verfahren geben, bei dem Ereignisprotokolle mithilfe ständiger und automatisierter Überwachungs- und Warnfunktionen oder manuell geprüft werden. Diese Prüfungen sollten mit einer bestimmten und dokumentierten Regelmäßigkeit durchgeführt werden, um Unregelmäßigkeiten zu erkennen und Abhilfemaßnahmen vorzuschlagen. | In Google Workspace sind Audit-Logs vorhanden, die Ihnen bei der Beantwortung folgender Fragen helfen: *Wer hat was getan? Wo und wann wurde es getan?* Zu den verfügbaren Audit-Logs zählen Admin-Aktivitätsprotokolle (Admin-Audit-Log), Sicherheitsprotokolle (Anmeldung, SAML und Access Transparency) sowie Nutzerdienste und Kontoprotokolle (E-Mail-Protokollsuche und Drive-Audit-Log). Im Hilfeartikel Verfügbare Audit-Logs erfahren Sie mehr darüber. Im Allgemeinen müssen Audit-Logs sechs Monate aufbewahrt werden. Weitere Informationen finden Sie unter Datenaufbewahrung und Zeitverzögerungen. Sie können anpassen, was in einem Audit-Log in der Google-Admin-Konsole angezeigt wird, indem Sie nach Nutzer oder Aktivität, Organisationseinheit oder Datum filtern. Außerdem lassen sich für bestimmte Aktivitäten Benachrichtigungen einrichten. |
| **Verschlüsselung** | Der Kunde sollte ermitteln, welche Daten gegebenenfalls verschlüsselt werden müssen und ob der genutzte Dienst über eine entsprechende Funktion verfügt. Der Kunde sollte die Verschlüsselung je nach Bedarf einsetzen, indem er die verfügbaren Tools verwendet. | Google Workspace-Kundendaten werden bei der Übertragung und Speicherung sowie auf Sicherungsmedien verschlüsselt. Verschlüsselung ist ein wichtiger Bestandteil der Google Workspace-Sicherheitsstrategie und trägt zum Schutz Ihrer E-Mails, Chats, Google Drive-Dateien und anderer Daten bei.<br><br>Weitere Informationen dazu, wie Daten bei der Speicherung, der Übertragung und auf Sicherungsmedien geschützt werden sowie Informationen zur Verwaltung von Verschlüsselungscodes finden Sie in unserem Google Workspace-Whitepaper zur Verschlüsselung.<br><br>Wenn Ihre Organisation eine zusätzliche Verschlüsselung von ausgehenden Nachrichten benötigt, können Sie als Administrator Regeln festlegen, die für ausgehende Nachrichten eine |

| | | |
|---|---|---|
| | | S/MIME-Signatur und -Verschlüsselung vorschreiben (Secure/Multipurpose Internet Mail Extensions). Damit sorgen Sie für eine angemessene Sicherheit, Vertraulichkeit und Integrität personenbezogener Kundendaten. |
| **Aufzeichnungen der Länder und Organisationen, in die gegebenenfalls personenidentifizierbare Informationen übertragen werden** | Der Kunde sollte die Länder, in die personenbezogene Kundendaten übertragen werden, kennen und diese für die Person zur Verfügung stellen können. Wenn diese Übertragung von einem Drittanbieter bzw. Verarbeiter durchgeführt wird, sollte der Kunde diese Informationen vom Verarbeiter beschaffen. | Google besitzt und betreibt Rechenzentren auf der ganzen Welt, damit seine Produkte rund um die Uhr abrufbereit sind. Weitere Informationen finden Sie unter Entdecken Sie die Standorte unserer Rechenzentren.<br><br>Sie können wählen, ob Ihre Daten an einem bestimmten Ort (die USA oder Europa) gespeichert werden sollen, wenn Sie hierzu eine Richtlinie für Speicherorte verwenden. Dieser Dienst bietet eine detaillierte Steuerung des Orts für die Speicherung von E-Mail-Nachrichten, Dokumenten und anderen Google Workspace-Inhalten. Lesen Sie unser Produktangebot zu Speicherorten aufmerksam und konsultieren Sie Ihren Rechtsberater, um selbst zu beurteilen, ob es Ihren spezifischen Compliance- oder Unternehmensanforderungen entspricht. |
| **Aufzeichnungen der Offenlegung personenidentifizierbarer Informationen für Dritte** | Der Kunde sollte Offenlegungen personenidentifizierbarer Informationen an Dritte aufzeichnen, einschließlich der Angaben für wen und wann diese Informationen offengelegt wurden. Dies kann auch Offenlegungen für Strafverfolgungsbehörden usw. umfassen. Wenn die Daten von einem Drittanbieter/Auftragsverarbeiter offengelegt werden, sollte der Kunde sicherstellen, dass dieser die entsprechenden Aufzeichnungen verwaltet, und diese je nach Bedarf beschaffen. | Google und die mit Google verbundenen Unternehmen nutzen bei der Bereitstellung ihrer Dienste verschiedene *Unterauftragsverarbeiter*. Weitere Informationen finden Sie unter Offenlegung von Google Workspace-Unterauftragsverarbeitern.<br><br>Als Administrator sollten Sie die Nutzung von Drittanbieter-Apps untersuchen. Sie haben die Option, Nutzer an der Installation von Drittanbieter-Apps zu hindern, wie beispielsweise Google Drive Apps und Add-ons zu Google Docs. Sie sollten die von Drittentwicklern stammende Sicherheitsdokumentation sowie die geltenden Datenverarbeitungsbedingungen prüfen, bevor Sie diese Apps mit Google Drive |

| | | |
|---|---|---|
| | | und Google Docs verwenden.<br><br>Wenn Google von Behörden ein Auskunftsersuchen für Cloud-Kundendaten erhält, sehen die Richtlinien von Google vor, dass die Behörde angewiesen wird, diese Daten direkt beim Cloud-Kunden anzufragen. Wir haben ein Team, dass solche Auskunftsersuchen prüft und sich vergewissert, dass sie allen rechtlichen Anforderungen entsprechen. Wenn Google zur Herausgabe von Daten gezwungen ist, informiert Google unverzüglich den Kunden vor der Offenlegung von Informationen, sofern eine solche Benachrichtigung nicht gesetzlich verboten ist oder ein lebensbedrohlicher Notfall besteht. Google wird soweit gesetzlich zulässig und gemäß den Bedingungen des jeweiligen Auskunftsersuchens den angemessenen Anforderungen von Kunden zur Erhebung von Einsprüchen gegen solche Ersuchen nachkommen.<br><br>Ausführliche Informationen finden Sie in unseremTransparenzbericht und im Google Cloud-Whitepaper zu Auskunftsersuchen von Behörden. |

| | | |
|---|---|---|
| **Ermittlung der Rechte betroffener Personen und Ermöglichung ihrer Ausübung (einschließlich Zugriff, Berichtigung, Löschen und Export)** | Der Kunde sollte mit den Anforderungen in Bezug auf die Rechte von Einzelpersonen vertraut sein, die sich auf die Verarbeitung ihrer personenbezogenen Kundendaten beziehen. Diese Rechte können etwa Zugriff, Berichtigung, Löschen und Export umfassen. Wenn der Kunde ein Drittanbietersystem nutzt, sollte er ermitteln, welche Teile des Systems (falls zutreffend) über Tools verfügen, die Einzelpersonen die Ausübung ihrer Rechte ermöglichen (z. B. den Zugriff auf ihre Daten). Wenn das System diese Funktionen bietet, sollte der Kunde sie je nach Bedarf einsetzen. | Als Google Workspace-Administrator können Sie mithilfe der Google Admin-Konsole mögliche Pflichten in Bezug auf die Anträge betroffener Personen erfüllen. Google Workspace bietet sowohl für Google Workspace-Admins als auch für betroffene Personen Funktionen, um direkt von Google-Produkten aus auf personenbezogene Kundendaten zuzugreifen und sie zu exportieren. Google Workspace-Administratoren können Daten mit dem Tool für den Datenexport auf Organisationsebene exportieren undGoogle Vault für gezielte nutzerbasierte Suchanfragen und Exporte verwenden. Betroffene Personen (Nutzer) können über die Benutzeroberfläche vonGoogle Datenexport selbst direkt auf personenbezogene Kundendaten zugreifen und diese exportieren. Eine Anleitung finden Sie imGoogle Workspace-Leitfaden zu Anträgen betroffener Personen. |
| **Aufbewahrung und Löschen** | Die Organisation, die personenidentifizierbare Informationen verarbeitet, muss dafür sorgen, dass sie diese Informationen je nach maßgeblicher Rechtsprechung nach einer bestimmten Zeitdauer löscht. | Google setzt beim Löschen der jeweiligen Kundendaten von den Google-Systemen Ihre Anweisungen als Administrator um. Admins können Nutzerkonten über die Google-Admin-Konsole verwalten. Dies unfasst auch das Löschen eines Kontos oder das Entfernen personenbezogener Kundendaten von Mobilgeräten und Produkten. Wenn Ihre Organisation Daten eine gewisse Zeit lang aufbewahren muss, können Sie Vault so konfigurieren, dass E-Mails und Dateien auch dann aufbewahrt werden, wenn Nutzer sie löschen und den Papierkorb leeren. Eine Anleitung zum Löschen von Einstellungen finden Sie im Google Workspace-Leitfaden zu Anträgen betroffener Personen. Weitere Informationen zu unserer Selbstverpflichtung finden Sie in Abschnitt 6 (Löschen von Daten) im Zusatz zur Datenverarbeitung.<br><br>In den Google Cloud-Datenschutzhinweisen finden Sie |

| | | |
|---|---|---|
| | | weitere Informationen zum Löschen und Aufbewahren von Dienstdaten. |
| **Endpunktverwaltung** | Der Kunde sollte dafür sorgen, dass die Verwendung von Mobilgeräten nicht die Sicherheit personenidentifizierbarer Informationen gefährdet. | Wenn Sie als Administrator die Google-Endpunktverwaltung verwenden, können Sie die Daten Ihrer Organisation auf den Mobilgeräten, Computern, Laptops und anderen Endpunkten Ihrer Nutzer noch sicherer machen. Mit der einfachen Verwaltung können Sie Sicherheitscodes erzwingen, Berichte zur Mobilgerätenutzung und einen Schutz vor Hackern einrichten, Kontodaten aus der Ferne löschen sowie Geräteprüfungen und Warnungen einrichten. Mit der erweiterten Verwaltung können Sie zusätzliche Sicherheits- und Datenschutzfunktionen wie etwa die Erzwingung starker Sicherheitscodes, das Blockieren gehackter Geräte und die Genehmigung von Geräten einrichten. Weitere Informationen sowie Hinweise zur Auswahl der passenden Version zur Geräteverwaltung finden Sie unter Funktionen der Mobilgeräteverwaltung im Vergleich. Mehr erfahren Sie außerdem in den Hilfeartikeln Einfache Mobilgeräteverwaltung einrichten und Erweiterte Mobilgeräteverwaltung einrichten. |

---

[1] Personenbezogene Kundendaten sind die in den Kundendaten enthaltenen personenbezogenen Daten.
[2] Kundendaten sind die Daten, die Sie, einschließlich Ihrer Organisation und ihrer Nutzer, Google beim Zugriff auf Google Workspace-Hauptdiensten zur Verfügung stellen, und die Daten, die Sie bei der Nutzung dieser Dienste erstellen.
[3] Dienstdaten sind personenbezogene Daten, die Google bei der Bereitstellung und Verwaltung von Cloud-Diensten erhebt oder generiert, mit Ausnahme von Kunden- und Partnerdaten. Dienstdaten unterliegen den Google Cloud-Datenschutzhinweisen.
[4] Siehe unsere ISO/IEC-Zertifizierungen (ISO/IEC 27001, 27017, 27701, 27018) sowie unseren SOC 3-Prüfbericht, der hier abgerufen werden kann. Für unsere Bestandskunden, die mehr über Sicherheit bei Google erfahren möchten, stellen wir gern einen detaillierten SOC 2-Bericht in der Übersicht über Complianceberichte bereit. Eine vollständige Auflistung aller unserer Compliance-Angebote finden Sie in unserem Center für Compliance-Ressourcen.
[5] G Suite for Education wird Schulen unter einer separaten G Suite for Education-Vereinbarung und gegebenenfalls gemäß dem Zusatz zur Datenverarbeitung zur Verfügung gestellt.

[6] Sollte die DSGVO für die Verarbeitung Ihrer Daten seitens Google gelten, muss Ihr Vertrag mit Google bestimmte Nutzungsbedingungen zur Datenverarbeitung enthalten. Dies ist beispielsweise der Fall, wenn Sie Ihren Sitz in der Europäischen Union haben oder außerhalb der Europäischen Union, aber Produkte/Dienstleistungen für betroffene Personen in der Europäischen Union anbieten.
[7] Sie müssen sich bei der Chrome-Verwaltung über die Cloud anmelden, um Gruppenrichtlinien für angemeldete Browser festzulegen.
[8] Für die Einrichtung eines Arbeitsprofils ist eine erweiterte Mobilgeräteverwaltung erforderlich. Weitere Informationen finden Sie unter Erweiterte Mobilgeräteverwaltung einrichten.
[9] Diese Funktion ist nur bei Google Workspace Enterprise Plus und G Suite Enterprise for Education verfügbar.