

Google Workspace Data Access Terms - Gmail Inbound And Google Drive

Bedingungen fuer Gmail-Readonly-Datenzugriff

Diese Bedingungen erlaeuern den Gmail-Inbound-Datenzugriff, den DynamicMail anfordert, wenn ein autorisierter Mandantenbenutzer oder Administrator Gmail fuer den Eingang von Mandantendokumenten verbindet.

Google-Sign-In-Identitaetsbereiche wie openid, email und profile sind von dieser Gmail-Datenzugriffs-Einwilligung getrennt. Eine Anmeldung mit Google bedeutet nicht, dass Gmail-Inbound-Zugriff akzeptiert wurde.

Angeforderter Scope

DynamicMail fordert <https://www.googleapis.com/auth/gmail.readonly> nur an, wenn ein autorisierter Mandantenbenutzer oder Administrator Gmail-Inbound-Dokumentenaufnahme verbindet. Dieser eingeschaenkte Gmail-Scope erlaubt DynamicMail, Gmail-Nachrichten und Einstellungen des verbundenen Google-Kontos anzusehen. DynamicMail verwendet den Scope fuer schreibgeschuetzte Inbound-Verarbeitung und nicht zum Senden, Aendern, Loeschen, Archivieren, Kennzeichnen oder Verschieben von Gmail-Nachrichten.

DynamicMail sollte keine Gmail-Daten anfordern oder verarbeiten, die nicht zur sichtbaren Inbound-Dokumentenaufnahmefunktion gehoeren.

Daten, auf die DynamicMail zugreifen kann

Wenn Gmail-Inbound verbunden ist, kann DynamicMail auf Gmail-Daten zugreifen, die erforderlich sind, um eingehende Geschaeftsdokumente zu finden und zu verarbeiten, einschliesslich:

- Nachrichten-IDs, Thread-IDs, History-IDs, Label-Referenzen und Synchronisationscursor;
- Absender, Empfaenger, Betreff, Datum, Header und andere Nachrichtenmetadaten;
- Nachrichtentexte und Snippets, die zur Erkennung des Dokumentkontexts benoetigt werden;
- Anhaenge und Inline-Dateien, die Rechnungen, Mitteilungen, Vereinbarungen, Quittungen oder andere Mandantendokumente enthalten koennen;
- Gmail-Einstellungen nur, soweit die Gmail API sie fuer den Readonly-Scope oder das Synchronisationsverhalten des Kontos erfordert;
- aus Gmail-Inhalten abgeleitete Daten, zum Beispiel geparste Dokumentfelder, OCR-Text, Klassifizierungslabls, Extraktionsergebnisse, Zusammenfassungen, Audit-

Ereignisse und Dokumentdatensätze.

Zweck

DynamicMail nutzt Gmail-Readonly-Daten, um die vom Mandanten ausgewählte Gmail-Inbound-Quelle bereitzustellen. Die vorgesehenen Zwecke sind:

- Erkennen eingehender Nachrichten, die Mandanten-Geschäftsdokumente enthalten können;
- Importieren von Anhängen oder Nachrichteninhalten, die der Mandant verarbeiten möchte;
- Extrahieren, Klassifizieren und Weiterleiten von Dokumenten in DynamicMail-Workflows;
- Abgleichen des Synchronisationsstatus, damit dieselbe Nachricht nicht wiederholt importiert wird;
- Anzeigen von Verbindungs-, Synchronisations- und Verarbeitungsstatus für autorisierte Mandantenbenutzer;
- Fehlerbehebung, Sicherheit, Audit und rechtliche Compliance-Aktivitäten, soweit dies nach den anwendbaren Richtlinien und der Mandantenvereinbarung zulässig ist.

DynamicMail darf Gmail-Daten nicht verkaufen, nicht für Werbung oder Retargeting verwenden, nicht an Datenbroker übertragen, nicht für Überwachung nutzen und nicht zur Bestimmung von Kreditwürdigkeit oder Kreditberechtigung verwenden.

Aufbewahrung

DynamicMail bewahrt aus Gmail abgeleitete Daten nur so lange auf, wie dies für die sichtbare Inbound-Dokumentenfunktion, Mandanten-

Dokumentaufbewahrungseinstellungen, Audit-Datensätze, Sicherheit, Streitbeilegung oder rechtliche Compliance erforderlich ist. OAuth-Tokens und

Synchronisationsmetadaten werden nur so lange aufbewahrt, wie sie für den Betrieb der verbundenen Gmail-Inbound-Quelle oder zur Wahrung erforderlicher Audit-Datensätze benötigt werden.

Rohe Gmail-Nachrichteninhalte, Anhänge und abgeleitete Dokumentdaten sollten gelöscht oder anonymisiert werden, wenn sie für den offengelegten Zweck nicht mehr benötigt werden, es sei denn, eine rechtliche, sicherheitsbezogene, Audit- oder Mandantenaufbewahrungspflicht erfordert die weitere Aufbewahrung.

Loeschung

Ein autorisierter Mandantenbenutzer oder Administrator kann die Löschung von zwischengespeicherten Google-abgeleiteten Daten, importierten Anhängen, extrahiertem Text und abgeleiteten Dokumentdatensätzen verlangen. DynamicMail

sollte die angeforderten Daten löschen oder anonymisieren, soweit dies nach den Aufbewahrungseinstellungen des Mandanten und anwendbarem Recht zulaessig ist.

Das Löschen importierter DynamicMail-Datensätze löscht nicht notwendigerweise die ursprüngliche E-Mail oder den ursprünglichen Anhang in Gmail, weil der Gmail-Readonly-Scope DynamicMail keine Berechtigung gibt, Gmail-Nachrichten zu ändern oder zu löschen.

Widerruf und Trennung

Der Mandant kann Gmail-Inbound in DynamicMail trennen. Nach Trennung oder lokalem Widerruf der Einwilligung darf DynamicMail die gespeicherten OAuth-Tokens für Gmail-Inbound nicht mehr verwenden und darf keine weiteren Gmail-Nachrichten aus dem verbundenen Konto lesen.

Der Inhaber des Google-Kontos kann die App-Autorisierung auch in den Google-Kontoeinstellungen widerrufen. Wenn die Google-Autorisierung widerrufen wird, muss DynamicMail den Gmail-API-Zugriff beenden, sobald Token-Aktualisierung oder API-Aufrufe fehlschlagen, und die Verbindung sollte als getrennt oder als erneut zu verbinden angezeigt werden.

Ein lokaler Widerruf entfernt bereits importierte DynamicMail-Dokumente nicht automatisch. Diese Datensätze werden gemäß den obigen Löschungs- und Aufbewahrungsregeln behandelt.

KI, OCR und Extraktion

DynamicMail kann OCR, Parsing, Klassifizierung, Zusammenfassung und andere KI-unterstützte Verarbeitung auf aus Gmail abgeleiteten Nachrichteninhalten und Anhängen nur verwenden, um den sichtbaren Inbound-Dokumentenworkflow für den Mandanten bereitzustellen oder zu verbessern. Gmail-Daten und abgeleitete Daten dürfen nicht verwendet werden, um ein allgemeines Machine-Learning- oder KI-Modell ausserhalb der vom Mandanten angeforderten Funktion zu erstellen, zu trainieren oder zu verbessern.

KI-unterstützte Ergebnisse können falsch sein. DynamicMail sollte extrahierte Daten als Workflow-Ausgabe darstellen, die autorisierte Benutzer prüfen, korrigieren, genehmigen, ablehnen oder löschen können.

Supportzugriff

DynamicMail-Personal, Auftragnehmer oder Unterauftragsverarbeiter sollten bestimmte Gmail-Nachrichten, Anhänge, extrahierten Text oder abgeleitete Gmail-Daten nicht lesen, es sei denn, eine der folgenden Bedingungen trifft zu:

- Der Benutzer hat ausdrücklich Support angefordert, der Zugriff auf bestimmte Daten erfordert;

- der Zugriff ist fuer Sicherheitsuntersuchung, Missbrauchsvermeidung oder Vorfallsreaktion erforderlich;
- der Zugriff ist erforderlich, um Recht, rechtlichen Verfahren oder einer bindenden Mandantenanweisung zu entsprechen;
- die Daten sind fuer interne Abläufe aggregiert oder anonymisiert, und kein bestimmter Gmail-Inhalt eines Benutzers ist lesbar.

Supportzugriff sollte auf das erforderliche Mindestmass beschränkt, soweit praktikabel zeitlich begrenzt und fuer Auditierbarkeit protokolliert sein.

Es ist Implementierungs- und Lokalisierungsmaterial, keine abschliessende Rechtsberatung. Es darf nicht als Google-Bestaetigung, Freigabe durch externe Rechtsberatung oder produktive Restricted-Scope-Freigabe dargestellt werden, solange keine gesonderten Pruefnachweise vorliegen.

Referenzen

- DynamicMail Restricted-Scope-Vertrag:
Documentation/DynamicMail/LocalizedIntegrations/google-restricted-scope-compliance-contract-2026-06-02.md
- Google API Services User Data Policy: <https://developers.google.com/terms/api-services-user-data-policy>
- Google Workspace API user data and developer policy:
<https://developers.google.com/workspace/workspace-api-user-data-developer-policy>
- Gmail API scopes: <https://developers.google.com/workspace/gmail/api/auth/scopes>
- Google restricted-scope verification guidance:
<https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification>

Bedingungen fuer Google-Drive-Datenzugriff

Diese Bedingungen erläutern den Google-Drive-Datenzugriff, den DynamicMail anfordert, wenn ein autorisierter Mandantenbenutzer oder Administrator Google Drive fuer Mandanten-Dokumentenworkflows verbindet.

Google-Sign-In-Identitätsbereiche wie openid, email und profile sind von dieser Google-Drive-Datenzugriffs-Einwilligung getrennt. Eine Anmeldung mit Google bedeutet nicht, dass Google-Drive-Zugriff akzeptiert wurde.

Angeforderter Scope

DynamicMail fordert <https://www.googleapis.com/auth/drive> nur an, wenn ein autorisierter Mandantenbenutzer oder Administrator Google Drive fuer Mandanten-Dokumentenworkflows verbindet. Dies ist ein breiter eingeschränkter Drive-Scope, der DynamicMail erlauben kann, alle Dateien im verbundenen Google-Drive-Konto

anzusehen und zu verwalten, einschliesslich Dateien, die dem Benutzer gehoeren, mit dem Benutzer geteilten Dateien, Ordnern und Inhalten in geteilten Ablagen, die fuer dieses Konto verfuegbar sind.

DynamicMail muss den Drive-Scope nur fuer offengelegte, sichtbare Drive-Dokumentenworkflows verwenden, die der Mandant ausgewaehlt hat. DynamicMail sollte Drive-Daten, die nicht zum sichtbaren Drive-Dokumentenworkflow gehoeren, nicht anfordern, durchsuchen, kopieren, herunterladen, aendern, loeschen oder anderweitig verarbeiten.

Daten, auf die DynamicMail zugreifen kann

Wenn Google Drive verbunden ist, kann DynamicMail auf Drive-Daten zugreifen, die zur Bereitstellung des ausgewaehlten Mandantenworkflows erforderlich sind, einschliesslich:

- Datei-IDs, Namen, MIME-Typen, Pruefsummen, Groesse, Zeitstempel, Beschreibungen, Labels, Ordnerreferenzen, uebergeordnete Ordner und andere Dateimetadaten;
- Ordnermetadaten, Metadaten geteilter Ablagen und Such- oder Auflistungsergebnisse, die zum Auffinden von Mandantendokumenten benoetigt werden;
- Dateiinhalte, Vorschauen, Miniaturansichten, Exporte, Downloads, Uploads und erzeugte oder bearbeitete Dateinutzlasten;
- Freigabe- und Berechtigungsmetadaten, wenn sie benoetigt werden, um eine sichtbare Drive-Dateioperation anzuzeigen oder abzuschliessen;
- kontobezogene Drive-Zusammenfassungsinformationen, die zur Bestaetigung des verbundenen Kontos und des Verbindungsstatus benoetigt werden;
- gespeicherte Kopien oder zwischengespeicherte Auszuege von Drive-Dateien, die in DynamicMail importiert wurden;
- aus Drive-Dateien abgeleitete Daten, zum Beispiel OCR-Text, geparste Dokumentfelder, Klassifizierungslabls, Extraktionsergebnisse, Zusammenfassungen, Audit-Ereignisse und Dokumentdatensaetze.

Zweck

DynamicMail nutzt Google-Drive-Daten, um vom Mandanten ausgewaehlte Drive-Dokumentenworkflows bereitzustellen. Die vorgesehenen Zwecke sind:

- autorisierten Benutzern zu ermoeglichen, Drive als Dokumentenquelle oder -ziel zu verbinden;
- Mandanten-Geschaeftdokumente, die ueber den Produktablauf ausgewaehlt wurden, zu finden, aufzulisten, zu importieren, herunterzuladen, zu exportieren, hochzuladen oder zu aktualisieren;
- Drive-Dokumente in DynamicMail-Workflows zu extrahieren, zu klassifizieren und weiterzuleiten;

- Verbindungs-, Dateioptions-, Synchronisations- und Verarbeitungsstatus fuer autorisierte Mandantenbenutzer anzuzeigen;
- Audit-Datensaetze und betriebliche Protokolle zu fuehren, die belegen, welche Drive-Operation angefordert und abgeschlossen wurde;
- Fehlerbehebung, Sicherheit, Missbrauchsvermeidung, Streitbeilegung und rechtliche Compliance-Aktivitaeten durchzufuehren, soweit dies nach den anwendbaren Richtlinien und der Mandantenvereinbarung zulaessig ist.

DynamicMail darf Google-Drive-Daten nicht verkaufen, nicht fuer Werbung oder Retargeting verwenden, nicht an Datenbroker uebertragen, nicht fuer Ueberwachung nutzen und nicht zur Bestimmung von Kreditwuerdigkeit oder Kreditberechtigung verwenden.

Breiter Drive-Scope und engster Scope

Der Scope <https://www.googleapis.com/auth/drive> ist breit, weil er Zugriff auf alle Drive-Dateien erlauben kann, die fuer das verbundene Konto verfuegbar sind. DynamicMail muss diesen Scope als vorlaeufig behandeln, bis Produkt- und Compliance-Pruefung dokumentieren, warum engere Drive-Scopes fuer den implementierten Workflow nicht ausreichen.

Vor produktiver Nutzung sollte DynamicMail engere Drive-Scopes wie `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` oder `drive.appfolder` evaluieren. Wenn ein engerer Scope die sichtbare Funktion unterstuetzen kann, muessen der angeforderte Scope, Einwilligungsdatensaetze, OAuth-Konfiguration, Quellasset, gerendertes Asset und Tests vor der Freigabe aktualisiert werden.

Aufbewahrung

DynamicMail bewahrt aus Drive abgeleitete Daten nur so lange auf, wie dies fuer den sichtbaren Drive-Workflow, Mandanten-Dokumentaufbewahrungseinstellungen, Audit-Datensaetze, Sicherheit, Streitbeilegung oder rechtliche Compliance erforderlich ist. OAuth-Tokens und Drive-Operationsmetadaten werden nur so lange aufbewahrt, wie sie fuer den Betrieb der verbundenen Drive-Integration oder zur Wahrung erforderlicher Audit-Datensaetze benoetigt werden.

Drive-Dateiinhalte, zwischengespeicherte Dateien, Metadaten, OCR-Text, extrahierte Felder und abgeleitete Dokumentdaten sollten gelöscht oder anonymisiert werden, wenn sie fuer den offengelegten Zweck nicht mehr benoetigt werden, es sei denn, eine rechtliche, sicherheitsbezogene, Audit- oder Mandantenaufbewahrungspflicht erfordert die weitere Aufbewahrung.

Loeschung

Ein autorisierter Mandantenbenutzer oder Administrator kann die Loeschung von zwischengespeicherten Google-abgeleiteten Daten, importierten Drive-Dateien, extrahiertem Text und abgeleiteten Dokumentdatensaetzen verlangen. DynamicMail

sollte die angeforderten Daten löschen oder anonymisieren, soweit dies nach den Aufbewahrungseinstellungen des Mandanten und anwendbarem Recht zulaessig ist.

Das Löschen importierter DynamicMail-Datensätze löscht nicht notwendigerweise die ursprüngliche Datei in Google Drive. DynamicMail sollte ursprüngliche Drive-Dateien nur dann ändern, verschieben, in den Papierkorb legen oder löschen, wenn ein autorisierter Benutzer diese Drive-Aktion ausdrücklich über einen sichtbaren Produktworkflow anfordert und die Aktion nach Mandantenrichtlinie und anwendbarem Recht zulaessig ist.

Widerruf und Trennung

Der Mandant kann Google Drive in DynamicMail trennen. Nach Trennung oder lokalem Widerruf der Einwilligung darf DynamicMail gespeicherte OAuth-Tokens für Google Drive nicht mehr verwenden und darf keine weiteren Drive-Dateien aus dem verbundenen Konto lesen, schreiben, herunterladen, hochladen, ändern oder löschen.

Der Inhaber des Google-Kontos kann die App-Autorisierung auch in den Google-Kontoeinstellungen widerrufen. Wenn die Google-Autorisierung widerrufen wird, muss DynamicMail den Drive-API-Zugriff beenden, sobald Token-Aktualisierung oder API-Aufrufe fehlschlagen, und die Verbindung sollte als getrennt oder als erneut zu verbinden angezeigt werden.

Ein lokaler Widerruf entfernt bereits importierte DynamicMail-Dokumente nicht automatisch. Diese Datensätze werden gemäss den obigen Löschungs- und Aufbewahrungsregeln behandelt.

KI, OCR und Extraktion

DynamicMail kann OCR, Parsing, Klassifizierung, Zusammenfassung und andere KI-unterstützte Verarbeitung auf Drive-Dateiinhalten und Metadaten nur verwenden, um den sichtbaren Mandanten-Drive-Dokumentenworkflow bereitzustellen oder zu verbessern. Drive-Daten und abgeleitete Daten dürfen nicht verwendet werden, um ein allgemeines Machine-Learning- oder KI-Modell ausserhalb der vom Mandanten angeforderten Funktion zu erstellen, zu trainieren oder zu verbessern.

KI-unterstützte Ergebnisse können falsch sein. DynamicMail sollte extrahierte Daten als Workflow-Ausgabe darstellen, die autorisierte Benutzer prüfen, korrigieren, genehmigen, ablehnen oder löschen können.

Supportzugriff

DynamicMail-Personal, Auftragnehmer oder Unterauftragsverarbeiter sollten bestimmte Drive-Dateien, extrahierten Text, Dateimetadaten oder abgeleitete Drive-Daten nicht lesen, es sei denn, eine der folgenden Bedingungen trifft zu:

- Der Benutzer hat ausdrücklich Support angefordert, der Zugriff auf bestimmte Daten erfordert;

- der Zugriff ist fuer Sicherheitsuntersuchung, Missbrauchsvermeidung oder Vorfallsreaktion erforderlich;
- der Zugriff ist erforderlich, um Recht, rechtlichen Verfahren oder einer bindenden Mandantenanweisung zu entsprechen;
- die Daten sind fuer interne Abläufe aggregiert oder anonymisiert, und kein bestimmter Drive-Inhalt eines Benutzers ist lesbar.

Supportzugriff sollte auf das erforderliche Mindestmass beschränkt, soweit praktikabel zeitlich begrenzt und fuer Auditierbarkeit protokolliert sein.

Es ist Implementierungs- und Lokalisierungsmaterial, keine abschliessende Rechtsberatung. Es darf nicht als Google-Bestaetigung, Freigabe durch externe Rechtsberatung oder produktive Restricted-Scope-Freigabe dargestellt werden, solange keine gesonderten Pruefnachweise vorliegen.

Referenzen

- DynamicMail Restricted-Scope-Vertrag:
Documentation/DynamicMail/LocalizedIntegrations/google-restricted-scope-compliance-contract-2026-06-02.md
- Google API Services User Data Policy: <https://developers.google.com/terms/api-services-user-data-policy>
- Google Workspace API user data and developer policy:
<https://developers.google.com/workspace/workspace-api-user-data-developer-policy>
- Google Drive API scopes:
<https://developers.google.com/workspace/drive/api/guides/api-specific-auth>
- Google restricted-scope verification guidance:
<https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification>