Google Workspace Data Access Terms - Gmail Inbound And Google Drive

Bedingungen für Gmail-Readonly-Datenzugriff

Diese Bedingungen erklären den Gmail-Inbound-Datenzugriff, den DynamicMail anfordert, wenn ein autorisierter Mandantenbenutzer oder Administrator Gmail für die Verarbeitung eingehender Mandantendokumente verbindet.

Diese Bedingungen decken nur Gmail-Inbound ab. Sie fügen keine landesspezifische Rechtsberatung hinzu und ändern nicht die Datencontroller- oder Counsel-Review-Markierungen aus den genehmigten Eingaben.

Google-Sign-In-Identitätsscopes wie `openid`, `email` und `profile` sind von dieser Gmail-Datenzugriffseinwilligung 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 die Gmail-Inbound-Dokumentenaufnahme verbindet. Dieser eingeschränkte Gmail-Scope erlaubt DynamicMail, Nachrichten und Einstellungen des verbundenen Gmail-Kontos anzusehen. DynamicMail verwendet den Scope für reine Leseverarbeitung und verwendet ihn nicht, um Gmail-Nachrichten zu senden, zu ändern, zu löschen, zu archivieren, zu labeln oder zu verschieben.

DynamicMail darf Gmail-Daten nicht anfordern oder verarbeiten, die nicht zur sichtbaren Gmail-Inbound-Dokumentenaufnahme gehören.

Daten, auf die DynamicMail zugreifen kann

Wenn Gmail-Inbound verbunden ist, kann DynamicMail auf Gmail-Daten zugreifen, die zum Finden und Verarbeiten eingehender Geschäftsdokumente erforderlich sind, einschließlich:

- Nachrichten-IDs, Thread-IDs, History-IDs, Label-Referenzen und Sync-Cursors;
- Absender, Empfänger, Betreff, Datum, Header und andere Nachrichtenmetadaten;
- Nachrichtentexte und Ausschnitte, die zur Erkennung des Dokumentkontexts erforderlich sind;
- Anhänge und Inline-Dateien, die Rechnungen, Mitteilungen, Vereinbarungen, Belege oder andere Mandantendokumente enthalten können;

- Gmail-Einstellungen nur, soweit die Gmail API sie für den Readonly-Scope oder das Synchronisationsverhalten des Kontos erfordert;
- abgeleitete Daten aus Gmail-Inhalten, zum Beispiel OCR-Text, geparste Dokumentfelder, Klassifizierungslabels, Extraktionsergebnisse, Zusammenfassungen, Audit-Ereignisse und Dokumentdatensätze.

Zweck der Nutzung

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 Synchronisationsstands, damit dieselbe Nachricht nicht wiederholt importiert wird;
- Anzeigen von Verbindungs-, Sync- und Verarbeitungsstatus für autorisierte Mandantenbenutzer;
- Fehlerbehebung, Sicherheit, Audit und rechtliche Compliance-Aktivitäten, soweit sie durch die anwendbaren Richtlinien und die Mandantenvereinbarung erlaubt sind.

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

Aufbewahrung

DynamicMail bewahrt aus Gmail abgeleitete Daten nur so lange auf, wie es für die sichtbare Inbound-Dokumentenfunktion, Mandanten-Dokumentaufbewahrungseinstellungen, Audit-Datensätze, Sicherheit, Streitfallbearbeitung oder rechtliche Compliance erforderlich ist. OAuth-Token und Sync-Metadaten werden nur so lange aufbewahrt, wie sie für den Betrieb der verbundenen Gmail-Inbound-Quelle oder für erforderliche Audit-Datensätze benötigt werden.

Rohinhalte von Gmail-Nachrichten, Anhänge und abgeleitete Dokumentdaten sollten gelöscht oder anonymisiert werden, wenn sie für den offengelegten Zweck nicht mehr erforderlich sind, sofern keine rechtliche, Sicherheits-, Audit- oder Mandantenaufbewahrungspflicht eine weitere Aufbewahrung erfordert.

Löschung

Ein autorisierter Mandantenbenutzer oder Administrator kann die Löschung von zwischengespeicherten Google-abgeleiteten Daten, importierten Anhängen,

extrahiertem Text und abgeleiteten Dokumentdatensätzen anfordern. DynamicMail sollte die angeforderten Daten löschen oder anonymisieren, soweit dies durch die Aufbewahrungseinstellungen des Mandanten und anwendbares Recht erlaubt ist.

Das Löschen importierter DynamicMail-Datensätze löscht nicht zwingend die ursprüngliche E-Mail oder den ursprünglichen Anhang aus 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 der Trennung oder einem lokalen Einwilligungswiderruf darf DynamicMail gespeicherte OAuth-Token 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 stoppen, sobald Token-Aktualisierungen oder API-Aufrufe fehlschlagen, und die Verbindung sollte als getrennt oder als erneut verbindungspflichtig angezeigt werden.

Ein lokaler Widerruf entfernt bereits importierte DynamicMail-Dokumente nicht automatisch. Diese Datensätze werden nach den oben beschriebenen 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 einsetzen, um den sichtbaren Inbound-Dokumentenworkflow für den Mandanten bereitzustellen oder zu verbessern. Gmail-Daten und daraus 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 nach dem Produktablauf prüfen, korrigieren, genehmigen, ablehnen oder löschen können.

Supportzugriff und menschlicher Zugriff

Personal, Auftragnehmer oder Unterauftragsverarbeiter von DynamicMail sollten bestimmte Gmail-Nachrichten, Anhänge, extrahierten Text oder abgeleitete Gmail-Daten nicht lesen, außer eine der folgenden Bedingungen liegt vor:

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

- der Zugriff ist für Sicherheitsuntersuchung, Missbrauchsprävention oder Incident Response erforderlich;
- der Zugriff ist erforderlich, um Recht, rechtliche Verfahren oder eine bindende Mandantenanweisung einzuhalten;
- die Daten sind für interne Abläufe aggregiert oder anonymisiert und keine Gmail-Inhalte eines bestimmten Benutzers sind lesbar.

Supportzugriff sollte dem Least-Privilege-Prinzip folgen, soweit praktikabel zeitlich begrenzt sein und zur Auditierbarkeit protokolliert werden.

Es ist lokalisierter Implementierungs- und Review-Text, keine finale Rechtsberatung. Es darf ohne gesonderte Review-Nachweise nicht so dargestellt werden, als trage es eine Google-Billigung, externe Counsel-Freigabe oder produktive Restricted-Scope-Freigabe.

Referenzen

- DynamicMail Restricted-Scope Contract: `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 für Google-Drive-Datenzugriff

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

Diese Bedingungen decken nur Google Drive ab. Sie fügen keine landesspezifische Rechtsberatung hinzu und ändern nicht die Datencontroller- oder Counsel-Review-Markierungen aus den genehmigten Eingaben.

Google-Sign-In-Identitätsscopes wie `openid`, `email` und `profile` sind von dieser Google-Drive-Datenzugriffseinwilligung 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 für 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 des Benutzers, mit dem Benutzer geteilter Dateien, Ordner und für dieses Konto verfügbarer Shared-Drive-Inhalte.

DynamicMail muss den Drive-Scope nur für offengelegte, sichtbare Drive-Dokumentenworkflows verwenden, die der Mandant ausgewählt hat. DynamicMail sollte Drive-Daten, die nicht zum sichtbaren Drive-Dokumentenworkflow gehören, nicht anfordern, durchsuchen, kopieren, herunterladen, ändern, löschen oder anderweitig verarbeiten.

Daten, auf die DynamicMail zugreifen kann

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

- Datei-IDs, Namen, MIME-Typen, Prüfsummen, Größe, Zeitstempel, Beschreibungen, Labels, Ordnerreferenzen, übergeordnete Ordner und andere Dateimetadaten;
- Ordnermetadaten, Shared-Drive-Metadaten und Such- oder Listing-Ergebnisse, die zum Auffinden von Mandantendokumenten erforderlich sind;
- Dateiinhalte, Vorschauen, Miniaturansichten, Exporte, Downloads, Uploads und generierte oder bearbeitete Dateipayloads;
- Freigabe- und Berechtigungsmetadaten, wenn sie erforderlich sind, um einen sichtbaren Drive-Dateivorgang anzuzeigen oder abzuschließen;
- kontobezogene Drive-Zusammenfassungsinformationen, die zur Bestätigung des verbundenen Kontos und des Verbindungsstatus erforderlich sind;
- gespeicherte Kopien oder zwischengespeicherte Auszüge von Drive-Dateien, die in DynamicMail importiert wurden;
- abgeleitete Daten aus Drive-Dateien, zum Beispiel OCR-Text, geparste Dokumentfelder, Klassifizierungslabels, Extraktionsergebnisse, Zusammenfassungen, Audit-Ereignisse und Dokumentdatensätze.

Zweck der Nutzung

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

- autorisierten Benutzern zu ermöglichen, Drive als Dokumentenquelle oder Dokumentenziel zu verbinden;
- Mandanten-Geschäftsdokumente, die im Produktablauf ausgewählt wurden, zu finden, aufzulisten, zu importieren, herunterzuladen, zu exportieren, hochzuladen oder zu aktualisieren;
- Drive-Dokumente zu extrahieren, zu klassifizieren und in DynamicMail-Workflows weiterzuleiten;

- Verbindungs-, Dateivorgangs-, Sync- und Verarbeitungsstatus für autorisierte Mandantenbenutzer anzuzeigen;
- Audit-Datensätze und operative Protokolle zu pflegen, die nachweisen, welcher Drive-Vorgang angefordert und abgeschlossen wurde;
- Fehlerbehebung, Sicherheit, Missbrauchsprävention, Streitfallbearbeitung und rechtliche Compliance-Aktivitäten durchzuführen, soweit sie durch die anwendbaren Richtlinien und die Mandantenvereinbarung erlaubt sind.

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

Breiter Drive-Scope und Narrowest-Scope-Hinweis

Der Scope `https://www.googleapis.com/auth/drive` ist breit, weil er Zugriff auf alle Drive-Dateien erlauben kann, die dem verbundenen Konto zur Verfügung stehen. DynamicMail muss diesen Scope als vorläufig behandeln, bis Produkt- und Compliance-Review dokumentiert, warum engere Drive-Scopes für 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` bewerten. Wenn ein engerer Scope die sichtbare Funktion unterstützen kann, müssen der angeforderte Scope, Einwilligungsdatensätze, OAuth-Konfiguration, Source-Asset, gerendertes Asset und Tests vor der Freigabe aktualisiert werden.

Aufbewahrung

DynamicMail bewahrt aus Drive abgeleitete Daten nur so lange auf, wie es für den sichtbaren Drive-Workflow, Mandanten-Dokumentaufbewahrungseinstellungen, Audit-Datensätze, Sicherheit, Streitfallbearbeitung oder rechtliche Compliance erforderlich ist. OAuth-Token und Drive-Vorgangsmetadaten werden nur so lange aufbewahrt, wie sie für den Betrieb der verbundenen Drive-Integration oder für erforderliche Audit-Datensätze benötigt werden.

Drive-Dateiinhalte, zwischengespeicherte Dateien, Metadaten, OCR-Text, extrahierte Felder und abgeleitete Dokumentdaten sollten gelöscht oder anonymisiert werden, wenn sie für den offengelegten Zweck nicht mehr erforderlich sind, sofern keine rechtliche, Sicherheits-, Audit- oder Mandantenaufbewahrungspflicht eine weitere Aufbewahrung erfordert.

Löschung

Ein autorisierter Mandantenbenutzer oder Administrator kann die Löschung von zwischengespeicherten Google-abgeleiteten Daten, importierten Drive-Dateien, extrahiertem Text und abgeleiteten Dokumentdatensätzen anfordern. DynamicMail sollte

die angeforderten Daten löschen oder anonymisieren, soweit dies durch die Aufbewahrungseinstellungen des Mandanten und anwendbares Recht erlaubt ist.

Das Löschen importierter DynamicMail-Datensätze löscht nicht zwingend die ursprüngliche Datei aus 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 durch Mandantenrichtlinien und anwendbares Recht erlaubt ist.

Widerruf und Trennung

Der Mandant kann Google Drive in DynamicMail trennen. Nach der Trennung oder einem lokalen Einwilligungswiderruf darf DynamicMail gespeicherte OAuth-Token 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 stoppen, sobald Token-Aktualisierungen oder API-Aufrufe fehlschlagen, und die Verbindung sollte als getrennt oder als erneut verbindungspflichtig angezeigt werden.

Ein lokaler Widerruf entfernt bereits importierte DynamicMail-Dokumente nicht automatisch. Diese Datensätze werden nach den oben beschriebenen 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 einsetzen, um den sichtbaren Mandanten-Drive-Dokumentenworkflow bereitzustellen oder zu verbessern. Drive-Daten und daraus 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 nach dem Produktablauf prüfen, korrigieren, genehmigen, ablehnen oder löschen können.

Supportzugriff und menschlicher Zugriff

Personal, Auftragnehmer oder Unterauftragsverarbeiter von DynamicMail sollten bestimmte Drive-Dateien, extrahierten Text, Dateimetadaten oder abgeleitete Drive-Daten nicht lesen, außer eine der folgenden Bedingungen liegt vor:

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

- der Zugriff ist für Sicherheitsuntersuchung, Missbrauchsprävention oder Incident Response erforderlich;
- der Zugriff ist erforderlich, um Recht, rechtliche Verfahren oder eine bindende Mandantenanweisung einzuhalten;
- die Daten sind für interne Abläufe aggregiert oder anonymisiert und keine Drive-Inhalte eines bestimmten Benutzers sind lesbar.

Supportzugriff sollte dem Least-Privilege-Prinzip folgen, soweit praktikabel zeitlich begrenzt sein und zur Auditierbarkeit protokolliert werden.

Es ist lokalisierter Implementierungs- und Review-Text, keine finale Rechtsberatung. Es darf ohne gesonderte Review-Nachweise nicht so dargestellt werden, als trage es eine Google-Billigung, externe Counsel-Freigabe oder produktive Restricted-Scope-Freigabe.

Referenzen

- DynamicMail Restricted-Scope Contract: `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