DYNAMICMAIL GOOGLE WORKSPACE TERMS

Bedingungen fuer Gmail-Readonly-Datenzugriff

Diese Bedingungen erlaeutern 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 eingeschraenkte 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, Klassifizierungslabels, Extraktionsergebnisse, Zusammenfassungen, Audit-

Ereignisse und Dokumentdatensaetze.

Zweck

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

- Erkennen eingehender Nachrichten, die Mandanten-Geschaeftsdokumente enthalten koennen;
- Importieren von Anhaengen oder Nachrichteninhalten, die der Mandant verarbeiten moechte;
- 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 fuer autorisierte Mandantenbenutzer;
- Fehlerbehebung, Sicherheit, Audit und rechtliche Compliance-Aktivitaeten, soweit dies nach den anwendbaren Richtlinien und der Mandantenvereinbarung zulaessig ist.

DynamicMail darf Gmail-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.

Aufbewahrung

DynamicMail bewahrt aus Gmail abgeleitete Daten nur so lange auf, wie dies fuer die sichtbare Inbound-Dokumentenfunktion, Mandanten-Dokumentaufbewahrungseinstellungen, Audit-Datensaetze, Sicherheit, Streitbeilegung oder rechtliche Compliance erforderlich ist. OAuth-Tokens und Synchronisationsmetadaten werden nur so lange aufbewahrt, wie sie fuer den Betrieb der verbundenen Gmail-Inbound-Quelle oder zur Wahrung erforderlicher Audit-Datensaetze benoetigt werden.

Rohe Gmail-Nachrichteninhalte, Anhaenge und abgeleitete Dokumentdaten sollten geloescht 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 Anhaengen, extrahiertem Text und abgeleiteten Dokumentdatensaetzen verlangen. DynamicMail

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

Das Loeschen importierter DynamicMail-Datensaetze loescht nicht notwendigerweise die urspruengliche E-Mail oder den urspruenglichen Anhang in Gmail, weil der Gmail-Readonly-Scope DynamicMail keine Berechtigung gibt, Gmail-Nachrichten zu aendern oder zu loeschen.

Widerruf und Trennung

Der Mandant kann Gmail-Inbound in DynamicMail trennen. Nach Trennung oder lokalem Widerruf der Einwilligung darf DynamicMail die gespeicherten OAuth-Tokens fuer 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 Datensaetze werden gemaess den obigen Loeschungs- und Aufbewahrungsregeln behandelt.

KI, OCR und Extraktion

DynamicMail kann OCR, Parsing, Klassifizierung, Zusammenfassung und andere KI-unterstuetzte Verarbeitung auf aus Gmail abgeleiteten Nachrichteninhalten und Anhaengen nur verwenden, um den sichtbaren Inbound-Dokumentenworkflow fuer den Mandanten bereitzustellen oder zu verbessern. Gmail-Daten und abgeleitete Daten duerfen 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-unterstuetzte Ergebnisse koennen falsch sein. DynamicMail sollte extrahierte Daten als Workflow-Ausgabe darstellen, die autorisierte Benutzer pruefen, korrigieren, genehmigen, ablehnen oder loeschen koennen.

Supportzugriff

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

- Der Benutzer hat ausdruecklich 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 Ablaufe aggregiert oder anonymisiert, und kein bestimmter Gmail-Inhalt eines Benutzers ist lesbar.

Supportzugriff sollte auf das erforderliche Mindestmass beschraenkt, 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