DYNAMICMAIL GOOGLE WORKSPACE TERMS

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