DYNAMICMAIL GOOGLE WORKSPACE TERMS

Bedingungen fuer Google-Drive-Datenzugriff

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

Google-Sign-In-Identitaetsbereiche 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 eingeschraenkter 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, Klassifizierungslabels, 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-Geschaeftsdokumente, 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-, Dateioperations-, 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 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 Drive-Dateien, 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 Datei in Google Drive. DynamicMail sollte urspruengliche Drive-Dateien nur dann aendern, verschieben, in den Papierkorb legen oder loeschen, wenn ein autorisierter Benutzer diese Drive-Aktion ausdruecklich ueber 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 fuer Google Drive nicht mehr verwenden und darf keine weiteren Drive-Dateien aus dem verbundenen Konto lesen, schreiben, herunterladen, hochladen, aendern oder loeschen.

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 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 Drive-Dateiinhalten und Metadaten nur verwenden, um den sichtbaren Mandanten-Drive-Dokumentenworkflow bereitzustellen oder zu verbessern. Drive-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 Drive-Dateien, extrahierten Text, Dateimetadaten oder abgeleitete Drive-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 Drive-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
- 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