DYNAMICMAIL GOOGLE WORKSPACE TERMS

Bedingungen fuer Google-Drive-Datenzugriff

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

Google-Sign-In-Identitaetsscopes 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 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 des Benutzers, mit dem Benutzer geteilter Dateien, Ordner und fuer dieses Konto verfuegbarer Shared-Drive-Inhalte.

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, 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 Bestaetigung des verbundenen Kontos und des Verbindungsstatus erforderlich sind;

- gespeicherte Kopien oder zwischengespeicherte Auszuege 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 Dokumentdatensaetze.

Zweck der Nutzung

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

- autorisierten Benutzern zu ermoeglichen, Drive als Dokumentenquelle oder Dokumentenziel zu verbinden;
- Mandanten-Geschaeftsdokumente, die im Produktablauf ausgewaehlt 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 fuer autorisierte Mandantenbenutzer anzuzeigen;
- Audit-Datensaetze und operative Protokolle zu pflegen, die nachweisen, welcher Drive-Vorgang angefordert und abgeschlossen wurde;
- Fehlerbehebung, Sicherheit, Missbrauchspraevention, Streitfallbearbeitung und rechtliche Compliance-Aktivitaeten durchzufuehren, soweit sie durch die anwendbaren Richtlinien und die Mandantenvereinbarung erlaubt sind.

DynamicMail darf Google-Drive-Daten nicht verkaufen, nicht fuer Werbung oder Retargeting verwenden, nicht an Datenbroker uebertragen, nicht zur Ueberwachung verwenden und nicht zur Bestimmung von Kreditwuerdigkeit 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 Verfuegung stehen. DynamicMail muss diesen Scope als vorlaeufig behandeln, bis Produkt- und Compliance-Review dokumentiert, 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` bewerten. Wenn ein engerer Scope die sichtbare Funktion unterstuetzen kann, muessen der angeforderte Scope, Einwilligungsdatensaetze, 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 fuer den sichtbaren Drive-Workflow, Mandanten-Dokumentaufbewahrungseinstellungen, Audit-Datensaetze, Sicherheit, Streitfallbearbeitung oder rechtliche Compliance erforderlich ist. OAuth-Token und Drive-Vorgangsmetadaten werden nur so lange aufbewahrt, wie sie fuer den Betrieb der verbundenen Drive-Integration oder fuer erforderliche 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 erforderlich sind, sofern keine rechtliche, Sicherheits-, Audit- oder Mandantenaufbewahrungspflicht eine weitere Aufbewahrung erfordert.

Loeschung

Ein autorisierter Mandantenbenutzer oder Administrator kann die Loeschung von zwischengespeicherten Google-abgeleiteten Daten, importierten Drive-Dateien, extrahiertem Text und abgeleiteten Dokumentdatensaetzen anfordern. DynamicMail sollte die angeforderten Daten loeschen oder anonymisieren, soweit dies durch die Aufbewahrungseinstellungen des Mandanten und anwendbares Recht erlaubt ist.

Das Loeschen importierter DynamicMail-Datensaetze loescht nicht zwingend die urspruengliche Datei aus 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 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 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 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 Datensaetze werden nach den oben beschriebenen 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 einsetzen, um den sichtbaren Mandanten-Drive-Dokumentenworkflow bereitzustellen oder zu verbessern. Drive-Daten und daraus 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 nach dem Produktablauf pruefen, korrigieren, genehmigen, ablehnen oder loeschen koennen.

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 ausdruecklich Support angefordert, der Zugriff auf bestimmte Daten erfordert;
- der Zugriff ist fuer Sicherheitsuntersuchung, Missbrauchspraevention oder Incident Response erforderlich;
- der Zugriff ist erforderlich, um Recht, rechtliche Verfahren oder eine bindende Mandantenanweisung einzuhalten;
- die Daten sind fuer interne Ablaeufe 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