Google Workspace Data Access Terms - Gmail Inbound And Google Drive

Termini di accesso ai dati Gmail in sola lettura

Questi termini spiegano l'accesso Gmail inbound che DynamicMail richiede quando un utente o amministratore autorizzato dell'organizzazione cliente collega Gmail per l'acquisizione di documenti in entrata.

Questo documento riguarda solo Gmail inbound. Non deve essere usato come termini completi di accesso ai dati Google Workspace per Google Drive.

Ambito

DynamicMail richiede `https://www.googleapis.com/auth/gmail.readonly` solo quando un utente o amministratore autorizzato dell'organizzazione cliente collega Gmail inbound per l'acquisizione di documenti. L'ambito consente a DynamicMail di visualizzare i messaggi e le impostazioni Gmail dell'account Google collegato. DynamicMail usa l'ambito per l'elaborazione in entrata in sola lettura e non lo usa per inviare, modificare, eliminare, archiviare, etichettare o spostare messaggi Gmail.

Gli ambiti di identità Google Sign-In, come `openid`, `email` e `profile`, sono separati da questo consenso di accesso ai dati Gmail. Accedere con Google non equivale ad accettare l'accesso Gmail inbound.

Dati a cui DynamicMail può accedere

Quando Gmail inbound è collegato, DynamicMail può accedere ai dati Gmail necessari per trovare ed elaborare documenti aziendali in entrata, inclusi:

- ID dei messaggi, ID dei thread, ID della cronologia, riferimenti alle etichette e cursori di sincronizzazione;
- mittente, destinatario, oggetto, data, intestazioni e altri metadati dei messaggi;
- corpi dei messaggi e snippet necessari per identificare il contesto del documento;
- allegati e file inline che possono contenere fatture, avvisi, accordi, ricevute o altri documenti dell'organizzazione cliente;
- impostazioni Gmail solo quando l'API Gmail le richiede per l'ambito readonly o per il comportamento di sincronizzazione dell'account;
- dati derivati creati dal contenuto Gmail, come testo OCR, campi documento analizzati, etichette di classificazione, risultati di estrazione, riepiloghi, eventi di audit e record documentali.

DynamicMail non dovrebbe richiedere o trattare dati Gmail non collegati alla funzionalità visibile di acquisizione documenti in entrata.

Finalità

DynamicMail usa i dati Gmail in sola lettura per fornire la sorgente Gmail inbound selezionata dall'organizzazione cliente. Le finalità previste sono:

- rilevare messaggi in entrata che possono contenere documenti aziendali dell'organizzazione cliente;
- importare allegati o contenuti dei messaggi che l'organizzazione cliente sceglie di elaborare;
- estrarre, classificare e indirizzare documenti nei flussi di lavoro DynamicMail;
- riconciliare lo stato di sincronizzazione affinche lo stesso messaggio non venga importato ripetutamente;
- mostrare lo stato di connessione, sincronizzazione ed elaborazione agli utenti autorizzati dell'organizzazione cliente;
- svolgere attività di supporto, sicurezza, audit e conformità legale consentite dalle policy applicabili e dall'accordo con l'organizzazione cliente.

DynamicMail non deve vendere dati Gmail, usarli per pubblicità o retargeting, trasferirli a broker di dati, usarli per sorveglianza o usarli per determinare affidabilità creditizia o idoneità a prestiti.

Conservazione

DynamicMail conserva i dati derivati da Gmail solo per il tempo necessario alla funzionalità visibile di acquisizione documenti in entrata, alle impostazioni di conservazione dei documenti dell'organizzazione cliente, ai record di audit, alla sicurezza, alla gestione delle controversie o alla conformità legale. I token OAuth e i metadati di sincronizzazione sono conservati solo finché sono necessari per operare la sorgente Gmail inbound collegata o per preservare i record di audit richiesti.

Il contenuto grezzo dei messaggi Gmail, gli allegati e i dati documentali derivati dovrebbero essere eliminati o anonimizzati quando non sono più necessari per la finalità dichiarata, salvo che un obbligo legale, di sicurezza, di audit o di conservazione dell'organizzazione cliente richieda una conservazione ulteriore.

Eliminazione

Un utente o amministratore autorizzato dell'organizzazione cliente può richiedere l'eliminazione dei dati derivati da Google memorizzati nella cache, degli allegati importati, del testo estratto e dei record documentali derivati. DynamicMail dovrebbe eliminare o anonimizzare i dati richiesti quando consentito dalle impostazioni di conservazione dell'organizzazione cliente e dal diritto applicabile.

L'eliminazione dei record importati in DynamicMail non elimina necessariamente l'e-mail o l'allegato originale da Gmail, perché l'ambito Gmail readonly non concede a DynamicMail l'autorizzazione a modificare o eliminare messaggi Gmail.

Revoca e disconnessione

L'organizzazione cliente può disconnettere Gmail inbound in DynamicMail. Dopo la disconnessione o una revoca locale del consenso, DynamicMail deve smettere di usare i token OAuth memorizzati per Gmail inbound e deve smettere di leggere ulteriori messaggi Gmail dall'account collegato.

Il proprietario dell'account Google può anche revocare l'autorizzazione dell'app nelle impostazioni dell'account Google. Se l'autorizzazione Google viene revocata, DynamicMail deve interrompere l'accesso all'API Gmail quando il refresh dei token o le chiamate API non riescono, e la connessione dovrebbe essere mostrata come disconnessa o come richiedente una riconnessione.

La revoca locale non rimuove automaticamente i documenti DynamicMail già importati. Tali record sono gestiti tramite le regole di eliminazione e conservazione indicate sopra.

Uso di IA, OCR ed estrazione

DynamicMail può usare OCR, parsing, classificazione, riepilogo e altri trattamenti assistiti da IA sul contenuto dei messaggi e sugli allegati derivati da Gmail solo per fornire o migliorare il flusso visibile di acquisizione documenti in entrata per l'organizzazione cliente. I dati Gmail e i dati derivati non devono essere usati per creare, addestrare o migliorare un modello generale di machine learning o IA al di fuori della funzionalità richiesta dall'organizzazione cliente.

I risultati assistiti da IA possono essere errati. DynamicMail dovrebbe presentare i dati estratti come output del flusso di lavoro che gli utenti autorizzati possono rivedere, correggere, approvare, rifiutare o eliminare secondo il flusso del prodotto.

Accesso del supporto e accesso umano

Il personale, i collaboratori o i sub-responsabili di DynamicMail non dovrebbero leggere specifici messaggi Gmail, allegati, testo estratto o dati Gmail derivati, salvo che si applichi una delle seguenti condizioni:

- l'utente ha richiesto esplicitamente supporto che richiede l'accesso a dati specifici;
- l'accesso è necessario per un'indagine di sicurezza, prevenzione degli abusi o risposta a incidenti;
- l'accesso è necessario per rispettare la legge, un procedimento legale o un'istruzione vincolante dell'organizzazione cliente;
- i dati sono aggregati o anonimizzati per operazioni interne e nessun contenuto Gmail di uno specifico utente è leggibile.

L'accesso del supporto dovrebbe seguire il principio del privilegio minimo, essere limitato nel tempo ove praticabile ed essere registrato per finalità di audit.

Stato di revisione legale

È materiale di implementazione e localizzazione, non consulenza legale finale. Non deve essere presentato come se avesse approvazione di Google, approvazione di un consulente legale esterno o autorizzazione di produzione per ambiti ristretti senza prova distinta di revisione.

Riferimenti sorgente

- 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

Termini di accesso ai dati Google Drive

Questi termini spiegano l'accesso Google Drive che DynamicMail richiede quando un utente o amministratore autorizzato dell'organizzazione cliente collega Google Drive per i flussi di lavoro documentali dell'organizzazione cliente.

Questo documento riguarda solo Google Drive. È destinato a essere usato insieme ai termini Gmail in sola lettura della stessa famiglia di asset Google Workspace.

Ambito

DynamicMail richiede `https://www.googleapis.com/auth/drive` solo quando un utente o amministratore autorizzato dell'organizzazione cliente collega Google Drive per i flussi di lavoro documentali dell'organizzazione cliente. Si tratta di un ambito Drive ristretto ampio che può consentire a DynamicMail di visualizzare e gestire tutti i file nell'account Google Drive collegato, inclusi i file di proprietà dell'utente, i file condivisi con l'utente, le cartelle e il contenuto dei drive condivisi disponibili per tale account.

DynamicMail deve usare l'ambito Drive solo per flussi di lavoro documentali Drive visibili e dichiarati, selezionati dall'organizzazione cliente. Gli ambiti di identità Google Sign-In, come `openid`, `email` e `profile`, sono separati da questo consenso di accesso ai dati Drive. Accedere con Google non equivale ad accettare l'accesso Google Drive.

Dati a cui DynamicMail può accedere

Quando Google Drive è collegato, DynamicMail può accedere ai dati Drive necessari per fornire il flusso di lavoro selezionato dall'organizzazione cliente, inclusi:

- ID dei file, nomi, tipi MIME, checksum, dimensioni, timestamp, descrizioni, etichette, riferimenti alle cartelle, cartelle principali e altri metadati dei file;
- metadati delle cartelle, metadati dei drive condivisi e risultati di ricerca o elenco necessari per localizzare i documenti dell'organizzazione cliente;
- contenuto dei file, anteprime, miniature, esportazioni, download, upload e payload di file generati o modificati;
- metadati di condivisione e autorizzazione quando necessari per mostrare o completare un'operazione Drive visibile su file;
- informazioni riepilogative a livello di account Drive necessarie per confermare l'account collegato e lo stato della connessione;
- copie memorizzate o estratti in cache di file Drive importati in DynamicMail;
- dati derivati creati dai file Drive, come testo OCR, campi documento analizzati, etichette di classificazione, risultati di estrazione, riepiloghi, eventi di audit e record documentali.

DynamicMail non dovrebbe richiedere, esplorare, copiare, scaricare, modificare, eliminare o trattare in altro modo dati Drive non collegati al flusso di lavoro documentale Drive visibile.

Finalità

DynamicMail usa i dati Google Drive per fornire i flussi di lavoro documentali Drive selezionati dall'organizzazione cliente. Le finalità previste sono:

- consentire agli utenti autorizzati di collegare Drive come sorgente o destinazione di documenti;
- trovare, elencare, importare, scaricare, esportare, caricare o aggiornare documenti aziendali dell'organizzazione cliente selezionati tramite il flusso del prodotto;
- estrarre, classificare e indirizzare documenti Drive nei flussi di lavoro DynamicMail;
- mostrare lo stato di connessione, operazione sui file, sincronizzazione ed elaborazione agli utenti autorizzati dell'organizzazione cliente;
- mantenere record di audit e log operativi che dimostrano quale operazione Drive è stata richiesta e completata;
- svolgere attività di supporto, sicurezza, prevenzione degli abusi, gestione delle controversie e conformità legale consentite dalle policy applicabili e dall'accordo con l'organizzazione cliente.

DynamicMail non deve vendere dati Google Drive, usarli per pubblicità o retargeting, trasferirli a broker di dati, usarli per sorveglianza o usarli per determinare affidabilità

creditizia o idoneità a prestiti.

Nota sull'ambito ampio e sull'ambito più ristretto

L'ambito `https://www.googleapis.com/auth/drive` è ampio perché può consentire l'accesso a tutti i file Drive disponibili per l'account collegato. DynamicMail deve trattare questo ambito come provvisorio fino a quando la revisione di prodotto e conformità documenta perché ambiti Drive più ristretti sono insufficienti per il flusso di lavoro implementato.

Prima dell'uso in produzione, DynamicMail dovrebbe valutare ambiti Drive più ristretti, come `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` o `drive.appfolder`. Se un ambito più ristretto può supportare la funzionalità visibile, l'ambito richiesto, i record di consenso, la configurazione OAuth, l'asset sorgente, l'asset renderizzato e i test devono essere aggiornati prima del rilascio.

Conservazione

DynamicMail conserva i dati derivati da Drive solo per il tempo necessario al flusso Drive visibile, alle impostazioni di conservazione dei documenti dell'organizzazione cliente, ai record di audit, alla sicurezza, alla gestione delle controversie o alla conformità legale. I token OAuth e i metadati delle operazioni Drive sono conservati solo finché sono necessari per operare l'integrazione Drive collegata o per preservare i record di audit richiesti.

Il contenuto dei file Drive, i file memorizzati nella cache, i metadati, il testo OCR, i campi estratti e i dati documentali derivati dovrebbero essere eliminati o anonimizzati quando non sono più necessari per la finalità dichiarata, salvo che un obbligo legale, di sicurezza, di audit o di conservazione dell'organizzazione cliente richieda una conservazione ulteriore.

Eliminazione

Un utente o amministratore autorizzato dell'organizzazione cliente può richiedere l'eliminazione dei dati derivati da Google memorizzati nella cache, dei file Drive importati, del testo estratto e dei record documentali derivati. DynamicMail dovrebbe eliminare o anonimizzare i dati richiesti quando consentito dalle impostazioni di conservazione dell'organizzazione cliente e dal diritto applicabile.

L'eliminazione dei record importati in DynamicMail non elimina necessariamente il file originale da Google Drive. DynamicMail dovrebbe modificare, spostare nel cestino o eliminare file Drive originali solo quando un utente autorizzato richiede esplicitamente tale azione Drive tramite un flusso di prodotto visibile e l'azione e consentita dalla policy dell'organizzazione cliente e dal diritto applicabile.

Revoca e disconnessione

L'organizzazione cliente può disconnettere Google Drive in DynamicMail. Dopo la disconnessione o una revoca locale del consenso, DynamicMail deve smettere di usare i

token OAuth memorizzati per Google Drive e deve smettere di leggere, scrivere, scaricare, caricare, modificare o eliminare ulteriori file Drive dall'account collegato.

Il proprietario dell'account Google può anche revocare l'autorizzazione dell'app nelle impostazioni dell'account Google. Se l'autorizzazione Google viene revocata, DynamicMail deve interrompere l'accesso all'API Drive quando il refresh dei token o le chiamate API non riescono, e la connessione dovrebbe essere mostrata come disconnessa o come richiedente una riconnessione.

La revoca locale non rimuove automaticamente i documenti DynamicMail già importati. Tali record sono gestiti tramite le regole di eliminazione e conservazione indicate sopra.

Uso di IA, OCR ed estrazione

DynamicMail può usare OCR, parsing, classificazione, riepilogo e altri trattamenti assistiti da IA sul contenuto e sui metadati dei file Drive solo per fornire o migliorare il flusso documentale Drive visibile dell'organizzazione cliente. I dati Drive e i dati derivati non devono essere usati per creare, addestrare o migliorare un modello generale di machine learning o IA al di fuori della funzionalità richiesta dall'organizzazione cliente.

I risultati assistiti da IA possono essere errati. DynamicMail dovrebbe presentare i dati estratti come output del flusso di lavoro che gli utenti autorizzati possono rivedere, correggere, approvare, rifiutare o eliminare secondo il flusso del prodotto.

Accesso del supporto e accesso umano

Il personale, i collaboratori o i sub-responsabili di DynamicMail non dovrebbero leggere specifici file Drive, testo estratto, metadati dei file o dati Drive derivati, salvo che si applichi una delle seguenti condizioni:

- l'utente ha richiesto esplicitamente supporto che richiede l'accesso a dati specifici;
- l'accesso è necessario per un'indagine di sicurezza, prevenzione degli abusi o risposta a incidenti;
- l'accesso è necessario per rispettare la legge, un procedimento legale o un'istruzione vincolante dell'organizzazione cliente;
- i dati sono aggregati o anonimizzati per operazioni interne e nessun contenuto Drive di uno specifico utente è leggibile.

L'accesso del supporto dovrebbe seguire il principio del privilegio minimo, essere limitato nel tempo ove praticabile ed essere registrato per finalità di audit.

Stato di revisione legale

È materiale di implementazione e localizzazione, non consulenza legale finale. Non deve essere presentato come se avesse approvazione di Google, approvazione di un consulente legale esterno o autorizzazione di produzione per ambiti ristretti senza prova distinta di revisione.

Riferimenti sorgente

- 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