

Google Workspace Data Access Terms - Gmail Inbound And Google Drive

Gmail Readonly Konditiounen fir den Datenzougrëff

Dës Konditiounen erklären de Gmail-Inbound-Zougrëff, deen DynamicMail ufreet, wann en autoriséierte Benotzer oder Administrateur vum Mandant Gmail fir d'Veaarbechtung vun erakommende Mandantendokumenten verbënnt.

Dëst Dokument deckt nëmme Gmail-Inbound of. Et däerf net als komplett Google Workspace Konditiounen fir den Datenzougrëff op Google Drive benotzt ginn.

Ugefrote Scope

DynamicMail freet <https://www.googleapis.com/auth/gmail.readonly> nëmmen un, wann en autoriséierte Benotzer oder Administrateur vum Mandant d'Gmail-Inbound-Dokumentenopnam verbënnt. Dës limitéierte Gmail-Scope erlaabt DynamicMail, Gmail-Noriichten an Astellung vum verbonnene Google-Konto ze kucken. DynamicMail benotzt de Scope fir liesnëmmen Inbound-Vearbechtung a benotzt en net, fir Gmail-Noriichten ze schécken, z'änneren, ze läschen, ze archivéieren, ze labelen oder ze verréckelen.

Google Sign-In Identitéits-Scopes wéi `openid`, `email` an `profile` si vun dëser Gmail-Datenzougrëffs-Zoustëmmung getrennt. Sech mat Google unzemellen heescht net, datt Gmail-Inbound-Zougrëff ugeholl gouf.

DynamicMail soll keng Gmail-Donnéeën ufroen oder veraarbechten, déi net zu der sichtbarer Gmail-Inbound-Dokumentenopnam gehéieren.

Donnéeën, op déi DynamicMail zougräife kann

Wann Gmail-Inbound verbonne gëtt, kann DynamicMail op déi Gmail-Donnéeën zougräifen, déi néideg sinn, fir erakommend Geschäftsdokumente ze fannen an ze veraarbechten, dorënner:

- Noriichten-IDen, Thread-IDen, History-IDen, Label-Referenzen a Synchronisatiouns-Cursoren;
- Ofsender, Empfänger, Betreff, Datum, Headeren an aner Noriichtemetadonnéeën;
- Noriichtekierper a Snippeten, déi néideg sinn, fir den Dokumentkontext z'erkennen;
- Annexen an inline Dateien, déi Rechnungen, Matdeelungen, Accorden, Quittungen oder aner Mandantendokumente enthalten kënnen;
- Gmail-Astellungen nëmme wann d'Gmail API se fir de Readonly-Scope oder fir d'Synchronisatiounsverhale vum Kont verlaangt;

- ofgeleet Donnéeën aus Gmail-Inhalter, zum Beispill OCR-Text, geparst Dokumentfelder, Klassifizierungslabellen, Extraktiounsresultater, Zesummefaassungen, Audit-Evenementer an Dokumentendatensätz.

Zweck vun der Notzung

DynamicMail benotzt Gmail-Readonly-Donnéeën, fir déi Gmail-Inbound-Quell bereetstellen, déi de Mandant ausgewielt huet. Déi virgesinn Zwecker sinn:

- erakommend Noriichten erkennen, déi Mandante-Geschäftsdokumenter enthalen kënnen;
- Annexen oder Noriichteninhalt importéieren, déi de Mandant veraarbechte wëllt;
- Dokumenter extrahéieren, klassifizéieren an an DynamicMail Workflows weiderleeden;
- de Synchronisationszoustand ofgläichen, fir datt déi selwecht Noriicht net ëmmer erëm importéiert gëtt;
- Verbindungs-, Synchronisations- a Veraarbechtungsstatus fir autoriséiert Mandantebenotzer weisen;
- Feelerbehebung, Sécherheet, Audit a rechtlech Compliance-Aktivitéiten duerchféieren, souwäit déi vun den uwendbare Richtlinnen an dem Mandantsaccord erlaabt sinn.

DynamicMail däerf Gmail-Donnéeën net verkafen, net fir Reklammen oder Retargeting benotzen, net un Datebroker iwwerdreen, net fir Iwwerwaachung benotzen an net benotzen, fir Kreditwierdegkeet oder Prêt-Berechtigung ze bestëmmen.

Opbewahrung

DynamicMail späichert aus Gmail ofgeleet Donnéeën nëmme soulaang wéi et fir déi sichtbar Inbound-Dokumentefunktioun, Mandanten-Dokumentopbewahrungsastellungen, Audit-Opzeechnungen, Sécherheet, Sträitbehandlung oder rechtlech Compliance néideg ass. OAuth-Token a Synchronisationsmetadonnéeë ginn nëmme soulaang gespäichert, wéi se fir de Betrib vun der verbonnener Gmail-Inbound-Quell oder fir erfuerderlech Audit-Opzeechnunge gebraucht ginn.

Rohe Gmail-Noriichteninhalter, Annexen an ofgeleet Dokumentendonnéeë solle gelöscht oder anonymiséiert ginn, wann se fir den offengeleeëne Zweck net méi néideg sinn, ausser eng rechtlech, Sécherheets-, Audit- oder Mandantenopbewahrungspflicht verlaangt eng weider Opbewahrung.

Läschen

En autoriséierte Benotzer oder Administrateur vum Mandant kann d'Läsche vu cached Google-ofgeleeenen Donnéeën, importéierten Annexen, extrahiertem Text an ofgeleeete Dokumentendatensätz ufroen. DynamicMail soll déi ugefrote Donnéeë läschen oder

anonymiséieren, souwäit d'Opbewahrungsastellunge vum Mandant an uwendbart Recht dat erlaben.

D'Läsche vun importéierten DynamicMail Datensätz läscht net onbedéngt déi ursprénglech E-Mail oder den Annex aus Gmail, well de Gmail-Readonly-Scope DynamicMail keng Erlaabnis gëtt, Gmail-Noriichten z'änneren oder ze läschen.

Widderruff an Trennen

De Mandant kann Gmail-Inbound an DynamicMail trennen. No enger Trennung oder engem lokale Widderruff vun der Zoustëmmung muss DynamicMail ophalen, gespäichert OAuth-Token fir Gmail-Inbound ze benotzen, a muss ophalen, weider Gmail-Noriichten aus dem verbonnene Kont ze liesen.

De Besëtzer vum Google-Konto kann d'App-Autorisatioun och an de Google-Kontastellungen widderruffen. Wann d'Google-Autorisatioun widderruff gëtt, muss DynamicMail de Gmail-API-Zougrëff stoppen, soubal Token-Erneuerungen oder API-Uruff feelschloen, an d'Verbindung soll als getrennt oder als nei ze verbannen ugewise ginn.

E lokale Widderruff läscht scho importéiert DynamicMail Dokumenter net automatesch. Déi Datensätz ginn no de Läschen- an Opbewahrungsregelen hei uewen behandelt.

AI, OCR an Extraktioun

DynamicMail kann OCR, Parsing, Klassifizéierung, Zesummefaassung an aner AI-ënnerstëtzt Veraarbechtung op aus Gmail ofgeleeten Noriichteninhalter an Annexen nëmme benotzen, fir de sichtbaren Inbound-Dokumenteworkflow fir de Mandant bereetzustellen oder ze verbesseren. Gmail-Donnéeën an ofgeleet Donnéeën däerfen net benotzt ginn, fir en allgemenge Machine-Learning- oder AI-Modell ausserhalb vun der vum Mandant ugefroter Funktioun ze erstellen, ze trainéieren oder ze verbesseren.

AI-ënnerstëtzt Resultater kënnen falsch sinn. DynamicMail soll extrahéiert Donnéeën als Workflow-Resultat weisen, dat autoriséiert Benotzer nom Produktfloss iwwerpräiwen, korrigéieren, geneemegen, refuséieren oder läsche kënnen.

Supportzougrëff a mënschlechen Zougrëff

Personal, Optraghueler oder Ënneroptragveraarbechter vun DynamicMail sollten spezifesch Gmail-Noriichten, Annexen, extrahéierten Text oder ofgeleet Gmail-Donnéeën net liesen, ausser eng vun dese Konditiounen gëllt:

- de Benotzer huet ausdrécklech Support gefrot, deen Zougrëff op spezifesch Donnéeën verlaangt;
- den Zougrëff ass néideg fir Sécherheetsënnersich, Mëssbrauchspräventioun oder Incident Response;
- den Zougrëff ass néideg, fir Recht, rechtlech Prozeduren oder eng bindend Mandantsuweisung anzehalen;

- d'Donnéeë si fir intern Operationen aggregéiert oder anonymiséiert, an et ass kee Gmail-Inhalt vun engem spezifische Benotzer liesbar.

Supportzougrëff soll dem Least-Privilege-Prinzip entsprechen, wou praktesch zäitlech limitéiert sinn, a fir Auditabilitéit protokolléiert ginn.

Et ass Implementéierungs- a Lokaliséierungsmaterial, keng final juristesche Berodung. Et däerf ouni separat Review-Nachweiser net esou duergestallt ginn, wéi wann et eng Google-Geneemegung, eng extern Counsel-Fräigab oder eng produktiv Restricted-Scope-Fräigab géif droen.

Quellreferenzen

- 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>

Google Drive Konditiounen fir den Datenzougrëff

Dës Konditiounen erklären de Google Drive Zougrëff, deen DynamicMail ufreet, wann en autoriséierte Benotzer oder Administrateur vum Mandant Google Drive fir Mandanten-Dokumenteworkflows verbënnt.

Dëst Dokument deckt nëmme Google Drive of. Et ass geduecht, zesumme mat de Gmail Readonly Konditiounen vun der selwechter Google Workspace Asset-Famill benotzt ze ginn.

Ugefrote Scope

DynamicMail freet <https://www.googleapis.com/auth/drive> nëmmen un, wann en autoriséierte Benotzer oder Administrateur vum Mandant Google Drive fir Mandanten-Dokumenteworkflows verbënnt. Dëst ass e breede limitéierte Drive-Scope, deen DynamicMail erlabe kann, all Dateien am verbonnene Google Drive Kont ze kucken an ze verwalten, dorënner Dateien, déi de Benotzer besëtzt, Dateien mat dem Benotzer gedeelt, Dossieren a Shared-Drive-Inhalter, déi fir dës Kont verfügbar sinn.

DynamicMail muss den Drive-Scope nëmme fir offengeleeën, sichtbar Drive-Dokumenteworkflows benotzen, déi de Mandant ausgewielt huet. Google Sign-In Identitéits-Scopes wéi openid, email an profile si vun dëser Drive-Datenzougrëffs-

Zoustëmmung getrennt. Sech mat Google unzemellen heescht net, datt Google Drive Zougrëff ugeholl gouf.

DynamicMail soll Drive-Donnéeën, déi net zum sichtbaren Drive-Dokumenteworkflow gehéieren, net ufroen, duerchsichen, kopéieren, eroflueden, änneren, läschen oder soss veraarbechten.

Donnéeën, op déi DynamicMail zougräife kann

Wann Google Drive verbonne gëtt, kann DynamicMail op déi Drive-Donnéeën zougräifen, déi néideg sinn, fir de vum Mandant ausgewielte Workflow bereetzustellen, dorënner:

- Datei-IDen, Nimm, MIME-Typen, Prüfsummen, Gréissten, Zäitstempelen, Beschreibungen, Labelen, Dossier-Referenzen, iwweruerdent Dossieren an aner Dateimetadonnéeën;
- Dossiermetadonnéeën, Shared-Drive-Metadonnéeën a Sich- oder Listing-Resultater, déi néideg sinn, fir Mandantendokumente ze lokaliséieren;
- Dateiinhalt, Virschauen, Miniaturen, Exporter, Downloads, Uploads a generéiert oder geännert Dateipayloaden;
- Deelen- a Berechtigungsmetadonnéeën, wann se néideg sinn, fir eng sichtbar Drive-Dateioperatioun ze weisen oder ofzeschléissen;
- Konto-bezungen Drive-Zesummefaassungsinformatiounen, déi néideg sinn, fir de verbonnene Kont an de Verbindungsstatus ze bestätegen;
- gespäichert Kopien oder cached Extraiten vu Drive-Dateien, déi an DynamicMail importéiert goufen;
- ofgeleet Donnéeën aus Drive-Dateien, zum Beispill OCR-Text, geparst Dokumentfelder, Klassifizierungslabellen, Extraktiounsresultater, Zesummefaassungen, Audit-Evenementer an Dokumentendatensätz.

Zweck vun der Notzung

DynamicMail benotzt Google Drive Donnéeën, fir déi Drive-Dokumenteworkflows bereetzustellen, déi de Mandant ausgewielt huet. Déi virgesinn Zwecker sinn:

- autoriséierte Benotzer erlaben, Drive als Dokumentequell oder Dokumentenzil ze verbannen;
- Mandante-Geschäftsdokumente, déi am Produktfloss ausgewielt goufen, fannen, oplëschen, importéieren, eroflueden, exportéieren, eroplueden oder aktualiséieren;
- Drive-Dokumente extrahéieren, klassifizéieren an an DynamicMail Workflows weiderleeden;
- Verbindungs-, Dateioperatiouns-, Synchronisatiouns- a Veraarbechtungsstatus fir autoriséiert Mandantebenotzer weisen;
- Audit-Opzeechnungen an operationell Logbicher féieren, déi nowisen, wéi eng Drive-Operatioun ugefrot an ofgeschloss gouf;

- Feelerbehebung, Sécherheet, Mössbrauchspräventioun, Sträitbehandlung a rechtlech Compliance-Aktivitéiten duerchféieren, souwäit déi vun den uwendbare Richtlinnen an dem Mandantsaccord erlaabt sinn.

DynamicMail däerf Google Drive Donnéeën net verkafen, net fir Reklammen oder Retargeting benotzen, net un Datebroker iwwerdroen, net fir Iwwerwaachung benotzen an net benotzen, fir Kreditwierdegkeet oder Prêt-Berechtigung ze bestëmmen.

Breede Drive-Scope an Narrowest-Scope-Hinweis

De Scope <https://www.googleapis.com/auth/drive> ass breet, well en Zougrëff op all Drive-Dateie erlaabt kann, déi dem verbundene Kont zur Verfügung stinn. DynamicMail muss dës Scope als provisoresch behandelen, bis Produkt- a Compliance-Review dokumentéiert, firwat méi eng Drive-Scopes fir den implementéierte Workflow net duergoen.

Virun enger produktiver Notzung soll DynamicMail méi eng Drive-Scopes wéi `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` oder `drive.appfolder` evaluéieren. Wann e méi eng Scope déi sichtbar Funktioun ënnerstëtze kann, mussen den ugefroten Scope, Zoustëmmungsopteechnungen, OAuth-Konfiguratioun, Source-Asset, gerendert Asset an Tester virun der Fräigab aktualiséiert ginn.

Opbewahrung

DynamicMail späichert aus Drive ofgeleet Donnéeën nëmme soulaang wéi et fir de sichtbaren Drive-Workflow, Mandanten-Dokumentopbewahrungsstellungen, Audit-Opteechnungen, Sécherheet, Sträitbehandlung oder rechtlech Compliance néideg ass. OAuth-Token an Drive-Operatiounsmetadonnéeën ginn nëmme soulaang gespäichert, wéi se fir de Betrib vun der verbundene Drive-Integratioun oder fir erforderlech Audit-Opteechnungen gebraucht ginn.

Drive-Dateiinhalter, cached Dateien, Metadonnéeën, OCR-Text, extrahéiert Felder an ofgeleet Dokumentendonnéeën solle gelöscht oder anonymiséiert ginn, wann se fir den offengeleeëne Zweck net méi néideg sinn, ausser eng rechtlech, Sécherheits-, Audit- oder Mandantenopbewahrungspflicht verlaangt eng weider Opbewahrung.

Läschen

En autoriséierte Benotzer oder Administrateur vum Mandant kann d'Läsche vu cached Google-ofgeleeeten Donnéeën, importéierten Drive-Dateien, extrahiertem Text an ofgeleeete Dokumentendatensätz ufroen. DynamicMail soll déi ugefroten Donnéeën läschen oder anonymiséieren, souwäit d'Opbewahrungsstellung vum Mandant an uwendbart Recht dat erlaben.

D'Läsche vun importéierten DynamicMail Datensätz löscht net onbedéngt déi ursprénglech Datei aus Google Drive. DynamicMail soll ursprénglech Drive-Dateien nëmmen änneren, verréckelen, an de Pabeierkuerf leeën oder läschen, wann en autoriséierte Benotzer dës Drive-Aktioun ausdrécklech iwwer e sichtbare

Produktworkflow ufreet an d'Aktioun duerch Mandantsrichtlinnen an uwendbart Recht erlaabt ass.

Widderruff an Trennen

De Mandant kann Google Drive an DynamicMail trennen. No enger Trennung oder engem lokale Widderruff vun der Zoustëmmung muss DynamicMail ophalen, gespäichert OAuth-Token fir Google Drive ze benotzen, a muss ophalen, weider Drive-Dateien aus dem verbundene Kont ze liesen, ze schreiwen, erofzelueden, eropzelueden, z'änneren oder ze läschen.

De Besëtzer vum Google-Konto kann d'App-Autorisatioun och an de Google-Kontstellungen widderruffen. Wann d'Google-Autorisatioun widderruff gëtt, muss DynamicMail den Drive-API-Zougrëff stoppen, soubal Token-Erneierungen oder API-Uruff feelschloen, an d'Verbindung soll als getrennt oder als nei ze verbannen ugewise ginn.

E lokale Widderruff läscht scho importéiert DynamicMail Dokumenter net automatesch. Déi Datensätz ginn no de Läschen- an Opbewahrungsregeln hei uewen behandelt.

AI, OCR an Extraktioun

DynamicMail kann OCR, Parsing, Klassifizierung, Zesummeffaassung an aner AI-ënnerstëtzt Veraarbechtung op Drive-Dateiinhalte a Metadonnéen nëmme benotzen, fir de sichtbare Mandanten-Drive-Dokumentenworkflow bereetstellen oder ze verbesseren. Drive-Donnéeen an ofgeleet Donnéeen däerfen net benotzt ginn, fir en allgemenge Machine-Learning- oder AI-Modell ausserhalb vun der vum Mandant ugefroter Funktioun ze erstellen, ze trainéieren oder ze verbesseren.

AI-ënnerstëtzt Resultater kënnen falsch sinn. DynamicMail soll extrahéiert Donnéeen als Workflow-Resultat weisen, dat autoriséiert Benotzer nom Produktfloss iwwerpréiwen, korrigéieren, geneemegen, refuséieren oder läsche kënnen.

Supportzougrëff a mënschlechen Zougrëff

Personal, Optraghueler oder Ënneroptragveraarbechter vun DynamicMail sollten spezifesch Drive-Dateien, extrahéierten Text, Dateimetadonnéen oder ofgeleet Drive-Donnéeen net liesen, ausser eng vun dese Konditiounen gëllt:

- de Benotzer huet ausdrécklech Support gefrot, deen Zougrëff op spezifesch Donnéeën verlaangt;
- den Zougrëff ass néideg fir Sécherheetsënnersich, Mëssbrauchspräventioun oder Incident Response;
- den Zougrëff ass néideg, fir Recht, rechtlech Prozeduren oder eng bindend Mandantsuweisung anzehalen;
- d'Donnéeën si fir intern Operatiounen aggregéiert oder anonymiséiert, an et ass kee Drive-Inhalt vun engem spezifesch Benotzer liesbar.

Supportzougrëff soll dem Least-Privilege-Prinzip entspriechen, wou praktesch zäitlech limitéiert sinn, a fir Auditabilitéit protokolléiert ginn.

Et ass Implementéierungs- a Lokaliséierungsmaterial, keng final juristesche Berodung. Et däerf ouni separat Review-Nachweiser net esou duergestallt ginn, wéi wann et eng Google-Geneemegung, eng extern Counsel-Fräigab oder eng produktiv Restricted-Scope-Fräigab géif droen.

Quellreferenzen

- 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>