Google Workspace Data Access Terms - Gmail Inbound And Google Drive

Gmail readonly voorwaarden voor beperkte-scope gegevensaccess

Deze voorwaarden leggen uit welke Gmail inbound-toegang DynamicMail vraagt wanneer een geautoriseerde tenantgebruiker of beheerder Gmail inbound documentinname koppelt.

Google Sign-In identiteits-scopes zoals `openid`, `email` en `profile` staan los van deze Gmail gegevensaccess-toestemming. Aanmelden met Google betekent niet dat Gmail inbound-toegang is aanvaard.

Scope

DynamicMail vraagt `https://www.googleapis.com/auth/gmail.readonly` alleen wanneer een geautoriseerde tenantgebruiker of beheerder Gmail inbound documentinname koppelt. De scope laat DynamicMail Gmail-berichten en instellingen voor het gekoppelde Google-account bekijken. DynamicMail gebruikt de scope voor alleen-lezen inboundverwerking en gebruikt deze niet om Gmail-berichten te verzenden, wijzigen, verwijderen, archiveren, labelen of verplaatsen.

DynamicMail mag geen Gmail-gegevens vragen of verwerken die geen verband houden met de zichtbare inbound documentinnamefunctie.

Gegevens waartoe DynamicMail toegang kan hebben

Wanneer Gmail inbound is gekoppeld, kan DynamicMail toegang hebben tot de Gmail-gegevens die nodig zijn om inkomende bedrijfsdocumenten te vinden en te verwerken, waaronder:

- bericht-ID's, thread-ID's, history-ID's, labelverwijzingen en synchronisatiecursors;
- afzender, ontvanger, onderwerp, datum, headers en andere berichtmetadata;
- berichtinhoud en snippets die nodig zijn om documentcontext te bepalen;
- bijlagen en inlinebestanden die facturen, kennisgevingen, overeenkomsten, ontvangstbewijzen of andere tenantdocumenten kunnen bevatten;
- Gmail-instellingen alleen waar de Gmail API die vereist voor de readonly scope of voor accountsynchronisatiegedrag;
- afgeleide gegevens uit Gmail-inhoud, zoals OCR-tekst, geparseerde documentvelden, classificatielabels, extractieresultaten, samenvattingen, auditgebeurtenissen en documentrecords.

Doel

DynamicMail gebruikt Gmail readonly-gegevens om de door de tenant geselecteerde Gmail inbound-bron te leveren. De beoogde doelen zijn:

- inkomende berichten detecteren die tenantbedrijfsdocumenten kunnen bevatten;
- bijlagen of berichtinhoud importeren die de tenant kiest om te verwerken;
- documenten extraheren, classificeren en routeren naar DynamicMail-workflows;
- synchronisatiestatus afstemmen zodat hetzelfde bericht niet herhaaldelijk wordt geimporteerd;
- verbindings-, synchronisatie- en verwerkingsstatus tonen aan geautoriseerde tenantgebruikers;
- troubleshooting, beveiliging, audit en wettelijke-nalevingsactiviteiten uitvoeren die zijn toegestaan door de toepasselijke beleidsregels en de tenantovereenkomst.

DynamicMail mag Gmail-gegevens niet verkopen, niet gebruiken voor advertenties of retargeting, niet overdragen aan databrokers, niet gebruiken voor surveillance en niet gebruiken om kredietwaardigheid of geschiktheid voor kredietverlening te bepalen.

Bewaring

DynamicMail bewaart Gmail-afgeleide gegevens alleen zolang dat nodig is voor de zichtbare inbound documentfunctie, tenantinstellingen voor documentbewaring, auditrecords, beveiliging, geschilafhandeling of wettelijke naleving. OAuth-tokens en synchronisatiemetadata worden alleen bewaard zolang dat nodig is om de gekoppelde Gmail inbound-bron te laten werken of om vereiste auditrecords te behouden.

Ruwe Gmail-berichtinhoud, bijlagen en afgeleide documentgegevens moeten worden verwijderd of geanonimiseerd wanneer ze niet langer nodig zijn voor het bekendgemaakte doel, tenzij een wettelijke, beveiligings-, audit- of tenantbewaringsverplichting verdere bewaring vereist.

Verwijdering

Een geautoriseerde tenantgebruiker of beheerder kan verwijdering vragen van Google-afgeleide gecachete gegevens, geimporteerde bijlagen, geextraheerde tekst en afgeleide documentrecords. DynamicMail zou de gevraagde gegevens moeten verwijderen of anonimiseren wanneer de tenantinstellingen voor bewaring en toepasselijke wetgeving dat toelaten.

Het verwijderen van geimporteerde DynamicMail-records verwijdert niet noodzakelijk het oorspronkelijke e-mailbericht of de oorspronkelijke bijlage uit Gmail, omdat de Gmail readonly-scope DynamicMail geen toestemming geeft om Gmail-berichten te wijzigen of te verwijderen.

Intrekking en loskoppeling

De tenant kan Gmail inbound in DynamicMail loskoppelen. Na loskoppeling of lokale intrekking van toestemming moet DynamicMail stoppen met het gebruiken van opgeslagen OAuth-tokens voor Gmail inbound en moet DynamicMail stoppen met het lezen van extra Gmail-berichten uit het gekoppelde account.

De eigenaar van het Google-account kan de app-autorisatie ook intrekken in de Google-accountinstellingen. Als Google-autorisatie wordt ingetrokken, moet DynamicMail stoppen met Gmail API-toegang wanneer tokenvernieuwing of API-aanroepen mislukken, en moet de verbinding worden getoond als losgekoppeld of als opnieuw koppelen vereist is.

Lokale intrekking verwijdert niet automatisch reeds geimporteerde DynamicMail-documenten. Die records worden behandeld volgens de verwijderings- en bewaringsregels hierboven.

AI, OCR en extractie

DynamicMail kan OCR, parsing, classificatie, samenvatting en andere AI-ondersteunde verwerking toepassen op Gmail-afgeleide berichtinhoud en bijlagen, alleen om de zichtbare inbound documentworkflow voor de tenant te leveren of te verbeteren. Gmail-gegevens en afgeleide gegevens mogen niet worden gebruikt om een algemeen machine-learning- of AI-model buiten de door de tenant gevraagde functie te maken, trainen of verbeteren.

AI-ondersteunde resultaten kunnen onjuist zijn. DynamicMail moet geextraheerde gegevens presenteren als workflowoutput die geautoriseerde gebruikers kunnen bekijken, corrigeren, goedkeuren, afwijzen of verwijderen volgens de productflow.

Support en menselijke toegang

DynamicMail-personeel, contractanten of subprocessors mogen specifieke Gmail-berichten, bijlagen, geextraheerde tekst of afgeleide Gmail-gegevens niet lezen, tenzij een van deze voorwaarden geldt:

- de gebruiker heeft expliciet om support gevraagd waarvoor toegang tot specifieke gegevens nodig is;
- toegang is nodig voor beveiligingsonderzoek, misbruikpreventie of incidentrespons;
- toegang is nodig om te voldoen aan wetgeving, juridisch proces of een bindende tenantinstructie;
- de gegevens zijn geaggregeerd of geanonimiseerd voor interne activiteiten en de Gmail-inhoud van een specifieke gebruiker is niet leesbaar.

Supporttoegang moet minimaal noodzakelijk zijn, waar praktisch tijdsbeperkt zijn en worden gelogd voor auditbaarheid.

Het is gelokaliseerd implementatie- en reviewmateriaal, geen definitief juridisch advies. Het mag niet worden gepresenteerd als bewijs van Google-goedkeuring, externe-juridische goedkeuring of productieclearance voor beperkte scopes zonder afzonderlijk beoordelingsbewijs.

Referenties

- 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 voorwaarden voor beperkte-scope gegevensaccess

Deze voorwaarden leggen uit welke Google Drive-toegang DynamicMail vraagt wanneer een geautoriseerde tenantgebruiker of beheerder Google Drive koppelt voor tenantdocumentworkflows.

Google Sign-In identiteits-scopes zoals `openid`, `email` en `profile` staan los van deze Google Drive gegevensaccess-toestemming. Aanmelden met Google betekent niet dat Google Drive-toegang is aanvaard.

Scope

DynamicMail vraagt `https://www.googleapis.com/auth/drive` alleen wanneer een geautoriseerde tenantgebruiker of beheerder Google Drive koppelt voor tenantdocumentworkflows. Dit is een brede restricted Drive-scope die DynamicMail kan toestaan alle bestanden in het gekoppelde Google Drive-account te bekijken en te beheren, waaronder bestanden waarvan de gebruiker eigenaar is, bestanden die met de gebruiker zijn gedeeld, mappen en shared-drive-inhoud die voor dat account beschikbaar is.

DynamicMail moet de Drive-scope alleen gebruiken voor bekendgemaakte, zichtbare Drive-documentworkflows die door de tenant zijn geselecteerd.

Gegevens waartoe DynamicMail toegang kan hebben

Wanneer Google Drive is gekoppeld, kan DynamicMail toegang hebben tot Drive-gegevens die nodig zijn om de geselecteerde tenantworkflow te leveren, waaronder:

- bestand-ID's, namen, MIME-types, checksums, grootte, tijdstempels, beschrijvingen, labels, mapverwijzingen, bovenliggende mappen en andere bestandsmetadata;
- mapmetadata, shared-drive-metadata en zoek- of lijstresultaten die nodig zijn om tenantdocumenten te vinden;
- bestandsinhoud, previews, thumbnails, exports, downloads, uploads en gegenereerde of bewerkte bestandspayloads;
- deel- en toestemmingsmetadata wanneer die nodig zijn om een zichtbare Drive-bestandsactie te tonen of te voltooien;
- accountniveau Drive-samenvattingsinformatie die nodig is om het gekoppelde account en de verbindingsstatus te bevestigen;
- opgeslagen kopieen of gecachete extracts van Drive-bestanden die in DynamicMail zijn geimporteerd;
- afgeleide gegevens uit Drive-bestanden, zoals OCR-tekst, geparseerde documentvelden, classificatielabels, extractieresultaten, samenvattingen, auditgebeurtenissen en documentrecords.

DynamicMail mag geen Drive-gegevens vragen, doorzoeken, kopieren, downloaden, wijzigen, verwijderen of anders verwerken die geen verband houden met de zichtbare Drive-documentworkflow.

Doel

DynamicMail gebruikt Google Drive-gegevens om door tenants geselecteerde Drive-documentworkflows te leveren. De beoogde doelen zijn:

- geautoriseerde gebruikers Drive laten koppelen als documentbron of documentbestemming;
- tenantbedrijfsdocumenten vinden, oplijsten, importeren, downloaden, exporteren, uploaden of bijwerken wanneer ze via de productflow zijn geselecteerd;
- Drive-documenten extraheren, classificeren en routeren naar DynamicMail-workflows;
- verbindings-, bestandsactie-, synchronisatie- en verwerkingsstatus tonen aan geautoriseerde tenantgebruikers;
- auditrecords en operationele logs bijhouden die aantonen welke Drive-actie is gevraagd en voltooid;
- troubleshooting, beveiliging, misbruikpreventie, geschilafhandeling en wettelijke-nalevingsactiviteiten uitvoeren die zijn toegestaan door de toepasselijke beleidsregels en de tenantovereenkomst.

DynamicMail mag Google Drive-gegevens niet verkopen, niet gebruiken voor advertenties of retargeting, niet overdragen aan databrokers, niet gebruiken voor surveillance en niet gebruiken om kredietwaardigheid of geschiktheid voor kredietverlening te bepalen.

Brede Drive-scope en nauwste scope

De `https://www.googleapis.com/auth/drive` scope is breed omdat deze toegang kan toestaan tot alle Drive-bestanden die beschikbaar zijn voor het gekoppelde account. DynamicMail moet deze scope als voorlopig behandelen totdat product- en compliancebeoordeling documenteert waarom nauwere Drive-scopes onvoldoende zijn voor de geimplementeerde workflow.

Voor productiegebruik moet DynamicMail nauwere Drive-scopes evalueren, zoals `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` of `drive.appfolder`. Als een nauwere scope de zichtbare functie kan ondersteunen, moeten de gevraagde scope, toestemmingsrecords, OAuth-configuratie, bronasset, gerenderd asset en tests voor release worden bijgewerkt.

Bewaring

DynamicMail bewaart Drive-afgeleide gegevens alleen zolang dat nodig is voor de zichtbare Drive-workflow, tenantinstellingen voor documentbewaring, auditrecords, beveiliging, geschilafhandeling of wettelijke naleving. OAuth-tokens en Drive-actiemetadata worden alleen bewaard zolang dat nodig is om de gekoppelde Drive-integratie te laten werken of vereiste auditrecords te behouden.

Drive-bestandsinhoud, gecachete bestanden, metadata, OCR-tekst, geextraheerde velden en afgeleide documentgegevens moeten worden verwijderd of geanonimiseerd wanneer ze niet langer nodig zijn voor het bekendgemaakte doel, tenzij een wettelijke, beveiligings-, audit- of tenantbewaringsverplichting verdere bewaring vereist.

Verwijdering

Een geautoriseerde tenantgebruiker of beheerder kan verwijdering vragen van Google-afgeleide gecachete gegevens, geimporteerde Drive-bestanden, geextraheerde tekst en afgeleide documentrecords. DynamicMail zou de gevraagde gegevens moeten verwijderen of anonimiseren wanneer de tenantinstellingen voor bewaring en toepasselijke wetgeving dat toelaten.

Het verwijderen van geimporteerde DynamicMail-records verwijdert niet noodzakelijk het oorspronkelijke bestand uit Google Drive. DynamicMail mag oorspronkelijke Drive-bestanden alleen wijzigen, verplaatsen, naar de prullenbak verplaatsen of verwijderen wanneer een geautoriseerde gebruiker die Drive-actie expliciet vraagt via een zichtbare productworkflow en de actie is toegestaan door tenantbeleid en toepasselijke wetgeving.

Intrekking en loskoppeling

De tenant kan Google Drive in DynamicMail loskoppelen. Na loskoppeling of lokale intrekking van toestemming moet DynamicMail stoppen met het gebruiken van opgeslagen OAuth-tokens voor Google Drive en moet DynamicMail stoppen met het lezen, schrijven, downloaden, uploaden, wijzigen of verwijderen van extra Drive-bestanden uit het gekoppelde account.

De eigenaar van het Google-account kan de app-autorisatie ook intrekken in de Google-accountinstellingen. Als Google-autorisatie wordt ingetrokken, moet DynamicMail stoppen met Drive API-toegang wanneer tokenvernieuwing of API-aanroepen mislukken, en moet de verbinding worden getoond als losgekoppeld of als opnieuw koppelen vereist is.

Lokale intrekking verwijdert niet automatisch reeds geimporteerde DynamicMail-documenten. Die records worden behandeld volgens de verwijderings- en bewaringsregels hierboven.

AI, OCR en extractie

DynamicMail kan OCR, parsing, classificatie, samenvatting en andere AI-ondersteunde verwerking toepassen op Drive-bestandsinhoud en metadata, alleen om de zichtbare tenant Drive-documentworkflow te leveren of te verbeteren. Drive-gegevens en afgeleide gegevens mogen niet worden gebruikt om een algemeen machine-learning- of AI-model buiten de door de tenant gevraagde functie te maken, trainen of verbeteren.

AI-ondersteunde resultaten kunnen onjuist zijn. DynamicMail moet geextraheerde gegevens presenteren als workflowoutput die geautoriseerde gebruikers kunnen bekijken, corrigeren, goedkeuren, afwijzen of verwijderen volgens de productflow.

Support en menselijke toegang

DynamicMail-personeel, contractanten of subprocessors mogen specifieke Drive-bestanden, geextraheerde tekst, bestandsmetadata of afgeleide Drive-gegevens niet lezen, tenzij een van deze voorwaarden geldt:

- de gebruiker heeft expliciet om support gevraagd waarvoor toegang tot specifieke gegevens nodig is;
- toegang is nodig voor beveiligingsonderzoek, misbruikpreventie of incidentrespons;
- toegang is nodig om te voldoen aan wetgeving, juridisch proces of een bindende tenantinstructie;
- de gegevens zijn geaggregeerd of geanonimiseerd voor interne activiteiten en de Drive-inhoud van een specifieke gebruiker is niet leesbaar.

Supporttoegang moet minimaal noodzakelijk zijn, waar praktisch tijdsbeperkt zijn en worden gelogd voor auditbaarheid.

Het is gelokaliseerd implementatie- en reviewmateriaal, geen definitief juridisch advies. Het mag niet worden gepresenteerd als bewijs van Google-goedkeuring, externe-juridische goedkeuring of productieclearance voor beperkte scopes zonder afzonderlijk beoordelingsbewijs.

Referenties

- 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