Google Workspace Data Access Terms - Gmail Inbound And Google Drive

Vilkår for Gmail Readonly-datatilgang

Desse vilkåra forklarar Gmail inbound-tilgangen som DynamicMail ber om når ein autorisert tenantbrukar eller administrator koplar Gmail inbound-dokumentinntak til dokumentarbeidsflytane til tenanten.

Google Sign-In-identitetsscope som `openid`, `email` og `profile` er skilde frå dette samtykket til Gmail-datatilgang. Innlogging med Google betyr ikkje at Gmail inbound-tilgang er akseptert.

Forespurt scope

DynamicMail ber berre om `https://www.googleapis.com/auth/gmail.readonly` når ein autorisert tenantbrukar eller administrator koplar Gmail inbound-dokumentinntak. Dette Gmail-scopet lèt DynamicMail sjå Gmail-meldingar og innstillingar for den tilkopla Google-kontoen. DynamicMail brukar scopet til skriveverna inbound-handsaming og brukar det ikkje til å sende, endre, slette, arkivere, merke eller flytte Gmail-meldingar.

DynamicMail skal ikkje be om eller behandle Gmail-data som ikkje er knytte til den synlege funksjonen for Gmail inbound-dokumentinntak.

Data DynamicMail kan få tilgang til

Når Gmail inbound er kopla til, kan DynamicMail få tilgang til Gmail-dataa som trengst for å finne og behandle innkomande forretningsdokument, inkludert:

- meldings-ID-ar, tråd-ID-ar, historikk-ID-ar, labelreferansar og synkroniseringsmarkørar;
- avsendar, mottakar, emne, dato, meldingshovud og andre meldingsmetadata;
- meldingsinnhald og utdrag som trengst for å identifisere dokumentkontekst;
- vedlegg og innebygde filer som kan innehalde fakturaer, varsel, avtalar, kvitteringar eller andre tenantdokument;
- Gmail-innstillingar berre der Gmail API-et krev dei for readonly-scopet eller synkroniseringsåtferda til kontoen;
- avleidde data oppretta frå Gmail-innhald, til dømes parsa dokumentfelt, OCR-tekst, klassifikasjonslabelar, uttrekksresultat, samandrag, audit-hendingar og dokumentpostar.

Kvifor DynamicMail brukar Gmail-data

DynamicMail brukar Gmail readonly-data for å levere Gmail inbound-kjelda som tenanten har valt. Dei tiltenkte føremåla er:

- å oppdage innkomande meldingar som kan innehalde forretningsdokumenta til tenanten;
- å importere vedlegg eller meldingsinnhald som tenanten vel å behandle;
- å trekkje ut, klassifisere og rute dokument inn i DynamicMail-arbeidsflytar;
- å avstemme synkroniseringstilstand slik at den same meldinga ikkje blir importert fleire gonger;
- å vise tilkoplings-, synkroniserings- og handsamingsstatus til autoriserte tenantbrukarar;
- feilsøking, tryggleik, audit og juridiske compliance-aktivitetar som er tillatne etter gjeldande policyar og tenantavtalen.

DynamicMail skal ikkje selje Gmail-data, bruke dei til annonsering eller retargeting, overføre dei til datameklarar, bruke dei til overvaking eller bruke dei til å fastslå kredittverdigheit eller lånerett.

Oppbevaring

DynamicMail oppbevarer Gmail-avleidde data berre så lenge det trengst for den synlege inbound-dokumentfunksjonen, innstillingane til tenanten for dokumentoppbevaring, auditpostar, tryggleik, tvisteløysing eller juridisk compliance. OAuth-token og synkroniseringsmetadata blir oppbevarte berre så lenge dei trengst for å drive den tilkopla Gmail inbound-kjelda eller bevare påkravde auditpostar.

Ubehandla Gmail-meldingsinnhald, vedlegg og avleidde dokumentdata bør slettast eller anonymiserast når dei ikkje lenger trengst for det opplyste føremålet, med mindre ei juridisk, tryggleiks-, audit- eller tenantoppbevaringsplikt krev vidare oppbevaring.

Sletting

Ein autorisert tenantbrukar eller administrator kan be om sletting av cachelagra Google-avleidde data, importerte vedlegg, uttrukken tekst og avleidde dokumentpostar. DynamicMail bør slette eller anonymisere dei forespurde dataa når det er tillate etter oppbevaringsinnstillingane til tenanten og gjeldande rett.

Sletting av importerte DynamicMail-postar slettar ikkje nødvendigvis den opphavlege e-posten eller vedlegget frå Gmail, fordi Gmail readonly-scopet ikkje gjev DynamicMail løyve til å endre eller slette Gmail-meldingar.

Tilbakekalling og fråkopling

Tenanten kan kople frå Gmail inbound i DynamicMail. Etter fråkopling eller lokal tilbakekalling av samtykke må DynamicMail slutte å bruke lagra OAuth-token for Gmail inbound og må slutte å lese fleire Gmail-meldingar frå den tilkopla kontoen.

Eigaren av Google-kontoen kan også tilbakekalle appautorisasjonen i Google-kontoinnstillingane. Dersom Google-autorisasjonen blir tilbakekalla, må DynamicMail stoppe Gmail API-tilgang når tokenoppdatering eller API-kall feilar, og tilkoplinga bør visast som fråkopla eller som krevjande ny tilkopling.

Lokal tilbakekalling fjernar ikkje automatisk DynamicMail-dokument som alt er importerte. Desse postane blir handterte etter reglane for sletting og oppbevaring ovanfor.

AI, OCR og uttrekk

DynamicMail kan bruke OCR, parsing, klassifisering, samandrag og anna AI-støtta handsaming av Gmail-avleidd meldingsinnhald og vedlegg berre for å levere eller forbetre den synlege inbound-dokumentarbeidsflyten for tenanten. Gmail-data og avleidde data skal ikkje brukast til å opprette, trene eller forbetre ein generell maskinlærings- eller AI-modell utanfor funksjonen som tenanten har bede om.

AI-støtta resultat kan vere feil. DynamicMail bør presentere uttrukne data som arbeidsflyt-output som autoriserte brukarar kan gjennomgå, rette, godkjenne, avvise eller slette i samsvar med produktflyten.

Support og menneskeleg tilgang

DynamicMail-personell, kontraktørar eller underdatabehandlarar bør ikkje lese spesifikke Gmail-meldingar, vedlegg, uttrukken tekst eller avleidde Gmail-data med mindre eitt av desse vilkåra gjeld:

- brukaren har uttrykkeleg bede om support som krev tilgang til spesifikke data;
- tilgangen er nødvendig for tryggleiksundersøking, førebygging av misbruk eller incident response;
- tilgangen er nødvendig for å overhalde rett, juridisk prosess eller ein bindande tenantinstruks;
- dataa er aggregerte eller anonymiserte for intern drift, og innhaldet frå Gmail til ingen spesifikk brukar er lesbart.

Supporttilgang bør vere basert på minste nødvendige rettar, vere tidsavgrensa der det er praktisk mogleg, og loggast for audit.

Det er lokalisert implementerings- og gjennomgangsmateriale, ikkje endeleg juridisk rådgjeving. Det må ikkje presenterast som om det har Google-godkjenning, godkjenning frå ekstern juridisk rådgjevar eller produksjonsklar restricted-scope-clearance utan separat gjennomgangsdokumentasjon.

Referansar

- 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

Vilkår for Google Drive-datatilgang

Desse vilkåra forklarar Google Drive-tilgangen som DynamicMail ber om når ein autorisert tenantbrukar eller administrator koplar Google Drive til dokumentarbeidsflytane til tenanten.

Google Sign-In-identitetsscope som `openid`, `email` og `profile` er skilde frå dette samtykket til Google Drive-datatilgang. Innlogging med Google betyr ikkje at Google Drive-tilgang er akseptert.

Forespurt scope

DynamicMail ber berre om `https://www.googleapis.com/auth/drive` når ein autorisert tenantbrukar eller administrator koplar Google Drive til dokumentarbeidsflytane til tenanten. Dette er eit breitt restricted Drive-scope som kan gje DynamicMail moglegheit til å sjå og administrere alle filer i den tilkopla Google Drive-kontoen, inkludert filer som brukaren eig, filer delte med brukaren, mapper og innhald i delte diskar som er tilgjengeleg for kontoen.

DynamicMail må berre bruke Drive-scopet til opplyste, synlege Drive-dokumentarbeidsflytar som tenanten har valt. DynamicMail bør ikkje be om, bla gjennom, kopiere, laste ned, endre, slette eller på annan måte behandle Drive-data som ikkje er knytte til den synlege Drive-dokumentarbeidsflyten.

Data DynamicMail kan få tilgang til

Når Google Drive er kopla til, kan DynamicMail få tilgang til Drive-dataa som trengst for å levere arbeidsflyten tenanten har valt, inkludert:

- fil-ID-ar, namn, MIME-typar, checksummar, storleik, tidsstempel, skildringar, labelar, mappereferansar, overordna mapper og andre filmetadata;
- mappemetadata, metadata for delte diskar og søkje- eller opplistingsresultat som trengst for å finne tenantdokument;
- filinnhald, førehandsvisingar, thumbnails, eksportar, nedlastingar, opplastingar og genererte eller redigerte filpayloadar;
- delings- og løyvemetadata når dei trengst for å vise eller fullføre ei synleg Drive-filhandling;

- kontoovergripande Drive-samandragsinformasjon som trengst for å stadfeste den tilkopla kontoen og tilkoplingsstatusen;
- lagra kopiar eller cachelagra uttrekk av Drive-filer som er importerte til DynamicMail;
- avleidde data oppretta frå Drive-filer, til dømes OCR-tekst, parsa dokumentfelt, klassifikasjonslabelar, uttrekksresultat, samandrag, audit-hendingar og dokumentpostar.

Føremål med bruken

DynamicMail brukar Google Drive-data for å levere Drive-dokumentarbeidsflytar som tenanten har valt. Dei tiltenkte føremåla er:

- å la autoriserte brukarar kople Drive som dokumentkjelde eller dokumentdestinasjon;
- å finne, liste, importere, laste ned, eksportere, laste opp eller oppdatere forretningsdokumenta til tenanten som er valde gjennom produktflyten;
- å trekkje ut, klassifisere og rute Drive-dokument inn i DynamicMail-arbeidsflytar;
- å vise tilkoplings-, filhandlings-, synkroniserings- og handsamingsstatus til autoriserte tenantbrukarar;
- å halde ved lag auditpostar og driftsloggar som dokumenterer kva Drive-handling som vart førespurd og fullført;
- feilsøking, tryggleik, førebygging av misbruk, tvisteløysing og juridiske compliance-aktivitetar som er tillatne etter gjeldande policyar og tenantavtalen.

DynamicMail skal ikkje selje Google Drive-data, bruke dei til annonsering eller retargeting, overføre dei til datameklarar, bruke dei til overvaking eller bruke dei til å fastslå kredittverdigheit eller lånerett.

Breitt Drive-scope og narrowest-scope-merknad

Scopet `https://www.googleapis.com/auth/drive` er breitt fordi det kan gje tilgang til alle Drive-filer som er tilgjengelege for den tilkopla kontoen. DynamicMail må behandle dette scopet som førebels til produkt- og compliance-gjennomgang dokumenterer kvifor smalare Drive-scopes ikkje er tilstrekkelege for den implementerte arbeidsflyten.

For produksjonsbruk bør DynamicMail evaluere smalare Drive-scopes som `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` eller `drive.appfolder`. Dersom eit smalare scope kan støtte den synlege funksjonen, må forespurt scope, samtykkepostar, OAuth-konfigurasjon, source asset, rendra asset og testar oppdaterast før release.

Oppbevaring

DynamicMail oppbevarer Drive-avleidde data berre så lenge det trengst for den synlege Drive-arbeidsflyten, innstillingane til tenanten for dokumentoppbevaring, auditpostar, tryggleik, tvisteløysing eller juridisk compliance. OAuth-token og Drive-handlingsmetadata blir oppbevarte berre så lenge dei trengst for å drive den tilkopla Drive-integrasjonen eller bevare påkravde auditpostar.

Drive-filinnhald, cachelagra filer, metadata, OCR-tekst, uttrukne felt og avleidde dokumentdata bør slettast eller anonymiserast når dei ikkje lenger trengst for det opplyste føremålet, med mindre ei juridisk, tryggleiks-, audit- eller tenantoppbevaringsplikt krev vidare oppbevaring.

Sletting

Ein autorisert tenantbrukar eller administrator kan be om sletting av cachelagra Google-avleidde data, importerte Drive-filer, uttrukken tekst og avleidde dokumentpostar. DynamicMail bør slette eller anonymisere dei forespurde dataa når det er tillate etter oppbevaringsinnstillingane til tenanten og gjeldande rett.

Sletting av importerte DynamicMail-postar slettar ikkje nødvendigvis den opphavlege fila frå Google Drive. DynamicMail bør berre endre, flytte, leggje i papirkorga eller slette opphavlege Drive-filer når ein autorisert brukar uttrykkeleg ber om den Drive-handlinga gjennom ein synleg produktarbeidsflyt, og handlinga er tillaten etter tenantpolicy og gjeldande rett.

Tilbakekalling og fråkopling

Tenanten kan kople frå Google Drive i DynamicMail. Etter fråkopling eller lokal tilbakekalling av samtykke må DynamicMail slutte å bruke lagra OAuth-token for Google Drive og må slutte å lese, skrive, laste ned, laste opp, endre eller slette fleire Drive-filer frå den tilkopla kontoen.

Eigaren av Google-kontoen kan også tilbakekalle appautorisasjonen i Google-kontoinnstillingane. Dersom Google-autorisasjonen blir tilbakekalla, må DynamicMail stoppe Drive API-tilgang når tokenoppdatering eller API-kall feilar, og tilkoplinga bør visast som fråkopla eller som krevjande ny tilkopling.

Lokal tilbakekalling fjernar ikkje automatisk DynamicMail-dokument som alt er importerte. Desse postane blir handterte etter reglane for sletting og oppbevaring ovanfor.

AI, OCR og uttrekk

DynamicMail kan bruke OCR, parsing, klassifisering, samandrag og anna AI-støtta handsaming av Drive-filinnhald og metadata berre for å levere eller forbetre den synlege Drive-dokumentarbeidsflyten for tenanten. Drive-data og avleidde data skal ikkje brukast til å opprette, trene eller forbetre ein generell maskinlærings- eller AI-modell utanfor funksjonen som tenanten har bede om.

AI-støtta resultat kan vere feil. DynamicMail bør presentere uttrukne data som arbeidsflyt-output som autoriserte brukarar kan gjennomgå, rette, godkjenne, avvise eller slette i samsvar med produktflyten.

Support og menneskeleg tilgang

DynamicMail-personell, kontraktørar eller underdatabehandlarar bør ikkje lese spesifikke Drive-filer, uttrukken tekst, filmetadata eller avleidde Drive-data med mindre eitt av desse vilkåra gjeld:

- brukaren har uttrykkeleg bede om support som krev tilgang til spesifikke data;
- tilgangen er nødvendig for tryggleiksundersøking, førebygging av misbruk eller incident response;
- tilgangen er nødvendig for å overhalde rett, juridisk prosess eller ein bindande tenantinstruks;
- dataa er aggregerte eller anonymiserte for intern drift, og innhaldet frå Drive til ingen spesifikk brukar er lesbart.

Supporttilgang bør vere basert på minste nødvendige rettar, vere tidsavgrensa der det er praktisk mogleg, og loggast for audit.

Det er lokalisert implementerings- og gjennomgangsmateriale, ikkje endeleg juridisk rådgjeving. Det må ikkje presenterast som om det har Google-godkjenning, godkjenning frå ekstern juridisk rådgjevar eller produksjonsklar restricted-scope-clearance utan separat gjennomgangsdokumentasjon.

Referansar

- 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