Google Workspace Data Access Terms - Gmail Inbound And Google Drive

Vilkår for Gmail Readonly-datatilgang

Disse vilkårene forklarer Gmail inbound-tilgangen som DynamicMail ber om når en autorisert tenantbruker eller administrator kobler Gmail inbound-dokumentinntak til tenantens dokumentworkflows.

Google Sign-In-identitetsscopes som `openid`, `email` og `profile` er atskilt fra dette samtykket til Gmail-datatilgang. Innlogging med Google betyr ikke at Gmail inbound-tilgang er akseptert.

Forespurt scope

DynamicMail ber bare om `https://www.googleapis.com/auth/gmail.readonly` når en autorisert tenantbruker eller administrator kobler Gmail inbound-dokumentinntak. Dette Gmail-scopet lar DynamicMail se Gmail-meldinger og innstillinger for den tilkoblede Google-kontoen. DynamicMail bruker scopet til skrivebeskyttet inbound-behandling og bruker det ikke til å sende, endre, slette, arkivere, merke eller flytte Gmail-meldinger.

DynamicMail skal ikke be om eller behandle Gmail-data som ikke er relatert til den synlige funksjonen for Gmail inbound-dokumentinntak.

Data DynamicMail kan få tilgang til

Når Gmail inbound er koblet til, kan DynamicMail få tilgang til Gmail-dataene som trengs for å finne og behandle innkommende forretningsdokumenter, inkludert:

- meldings-ID-er, tråd-ID-er, historikk-ID-er, labelreferanser og synkroniseringsmarkører;
- avsender, mottaker, emne, dato, headere og andre meldingsmetadata;
- meldingsinnhold og utdrag som trengs for å identifisere dokumentkontekst;
- vedlegg og inline-filer som kan inneholde fakturaer, varsler, avtaler, kvitteringer eller andre tenantdokumenter;
- Gmail-innstillinger bare der Gmail API-et krever dem for readonly-scopet eller kontoens synkroniseringsatferd;
- avledede data opprettet fra Gmail-innhold, for eksempel parsede dokumentfelter, OCR-tekst, klassifikasjonslabels, uttrekksresultater, sammendrag, audit-hendelser og dokumentposter.

Hvorfor DynamicMail bruker Gmail-data

DynamicMail bruker Gmail readonly-data for å levere Gmail inbound-kilden som tenanten har valgt. De tiltenkte formålene er:

- å oppdage innkommende meldinger som kan inneholde tenantens forretningsdokumenter;
- å importere vedlegg eller meldingsinnhold som tenanten velger å behandle;
- å trekke ut, klassifisere og rute dokumenter inn i DynamicMail-workflows;
- å avstemme synkroniseringstilstand slik at samme melding ikke importeres gjentatte ganger;
- å vise tilkoblings-, synkroniserings- og behandlingsstatus til autoriserte tenantbrukere;
- feilsøking, sikkerhet, audit og juridiske compliance-aktiviteter som er tillatt etter gjeldende policyer og tenantavtalen.

DynamicMail skal ikke selge Gmail-data, bruke dem til annonsering eller retargeting, overføre dem til datameglere, bruke dem til overvåking eller bruke dem til å fastslå kredittverdighet eller låneberettigelse.

Oppbevaring

DynamicMail oppbevarer Gmail-avledede data bare så lenge det trengs for den synlige inbound-dokumentfunksjonen, tenantens innstillinger for dokumentoppbevaring, auditposter, sikkerhet, tvisteløsing eller juridisk compliance. OAuth-tokens og synkroniseringsmetadata oppbevares bare så lenge de trengs for å drive den tilkoblede Gmail inbound-kilden eller bevare påkrevde auditposter.

Ubehandlet Gmail-meldingsinnhold, vedlegg og avledede dokumentdata bør slettes eller anonymiseres når de ikke lenger trengs for det opplyste formålet, med mindre en juridisk, sikkerhetsmessig, auditmessig eller tenantoppbevaringsmessig forpliktelse krever fortsatt oppbevaring.

Sletting

En autorisert tenantbruker eller administrator kan be om sletting av cachelagrede Google-avledede data, importerte vedlegg, uttrukket tekst og avledede dokumentposter. DynamicMail bør slette eller anonymisere de forespurte dataene når det er tillatt etter tenantens oppbevaringsinnstillinger og gjeldende rett.

Sletting av importerte DynamicMail-poster sletter ikke nødvendigvis den opprinnelige e-posten eller vedlegget fra Gmail, fordi Gmail readonly-scopet ikke gir DynamicMail tillatelse til å endre eller slette Gmail-meldinger.

Tilbakekalling og frakobling

Tenanten kan koble fra Gmail inbound i DynamicMail. Etter frakobling eller lokal tilbakekalling av samtykke må DynamicMail slutte å bruke lagrede OAuth-tokens for

Gmail inbound og må slutte å lese flere Gmail-meldinger fra den tilkoblede kontoen.

Eieren av Google-kontoen kan også tilbakekalle appens autorisasjon i Google-kontoinnstillingene. Hvis Google-autorisasjonen tilbakekalles, må DynamicMail stoppe Gmail API-tilgang når tokenoppdatering eller API-kall feiler, og tilkoblingen bør vises som frakoblet eller som krevende ny tilkobling.

Lokal tilbakekalling fjerner ikke automatisk allerede importerte DynamicMail-dokumenter. Disse postene håndteres etter reglene for sletting og oppbevaring ovenfor.

AI, OCR og uttrekk

DynamicMail kan bruke OCR, parsing, klassifisering, sammendrag og annen AI-støttet behandling av Gmail-avledet meldingsinnhold og vedlegg bare for å levere eller forbedre det synlige inbound-dokumentworkflowet for tenanten. Gmail-data og avledede data skal ikke brukes til å opprette, trene eller forbedre en generell maskinlærings- eller AI-modell utenfor funksjonen som tenanten har bedt om.

AI-støttede resultater kan være feil. DynamicMail bør presentere uttrukne data som workflow-output som autoriserte brukere kan gjennomgå, rette, godkjenne, avvise eller slette i henhold til produktflyten.

Support og menneskelig tilgang

DynamicMail-personell, kontraktører eller underdatabehandlere bør ikke lese spesifikke Gmail-meldinger, vedlegg, uttrukket tekst eller avledede Gmail-data med mindre ett av disse vilkårene gjelder:

- brukeren har uttrykkelig bedt om support som krever tilgang til spesifikke data;
- tilgangen er nødvendig for sikkerhetsundersøkelse, forebygging av misbruk eller incident response;
- tilgangen er nødvendig for å overholde rett, juridisk prosess eller en bindende tenantinstruks;
- dataene er aggregerte eller anonymiserte for intern drift, og ingen spesifikk brukers Gmail-innhold er lesbart.

Supporttilgang bør være basert på minste nødvendige rettigheter, være tidsbegrenset der det er praktisk mulig og logges for audit.

Det er lokalisert implementerings- og reviewmateriale, ikke endelig juridisk rådgivning. Det må ikke presenteres som om det har Google-godkjenning, godkjenning fra ekstern juridisk rådgiver eller produksjonsklar restricted-scope-clearance uten separat reviewdokumentasjon.

Referanser

- 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

Disse vilkårene forklarer Google Drive-tilgangen som DynamicMail ber om når en autorisert tenantbruker eller administrator kobler Google Drive til tenantens dokumentworkflows.

Google Sign-In-identitetsscopes som `openid`, `email` og `profile` er atskilt fra dette samtykket til Google Drive-datatilgang. Innlogging med Google betyr ikke at Google Drive-tilgang er akseptert.

Forespurt scope

DynamicMail ber bare om `https://www.googleapis.com/auth/drive` når en autorisert tenantbruker eller administrator kobler Google Drive til tenantens dokumentworkflows. Dette er et bredt restricted Drive-scope som kan gi DynamicMail mulighet til å se og administrere alle filer i den tilkoblede Google Drive-kontoen, inkludert filer som brukeren eier, filer delt med brukeren, mapper og innhold i delte disker som er tilgjengelig for kontoen.

DynamicMail må bare bruke Drive-scopet til opplyste, synlige Drive-dokumentworkflows som tenanten har valgt. DynamicMail bør ikke be om, bla gjennom, kopiere, laste ned, endre, slette eller på annen måte behandle Drive-data som ikke er relatert til det synlige Drive-dokumentworkflowet.

Data DynamicMail kan få tilgang til

Når Google Drive er koblet til, kan DynamicMail få tilgang til Drive-dataene som trengs for å levere workflowet tenanten har valgt, inkludert:

- fil-ID-er, navn, MIME-typer, checksums, størrelse, tidsstempler, beskrivelser, labels, mappereferanser, overordnede mapper og andre filmetadata;
- mappemetadata, metadata for delte disker og søke- eller listningsresultater som trengs for å finne tenantdokumenter;
- filinnhold, forhåndsvisninger, thumbnails, eksporter, nedlastinger, opplastinger og genererte eller redigerte filpayloads;

- delings- og tillatelsesmetadata når de trengs for å vise eller fullføre en synlig Drive-filhandling;
- kontoovergripende Drive-sammendragsinformasjon som trengs for å bekrefte den tilkoblede kontoen og tilkoblingsstatusen;
- lagrede kopier eller cachelagrede uttrekk av Drive-filer som er importert til DynamicMail;
- avledede data opprettet fra Drive-filer, for eksempel OCR-tekst, parsede dokumentfelter, klassifikasjonslabels, uttrekksresultater, sammendrag, audit-hendelser og dokumentposter.

Formål med bruken

DynamicMail bruker Google Drive-data for å levere Drive-dokumentworkflows som tenanten har valgt. De tiltenkte formålene er:

- å la autoriserte brukere koble Drive som dokumentkilde eller dokumentdestinasjon;
- å finne, liste, importere, laste ned, eksportere, laste opp eller oppdatere tenantens forretningsdokumenter som er valgt gjennom produktflyten;
- å trekke ut, klassifisere og rute Drive-dokumenter inn i DynamicMail-workflows;
- å vise tilkoblings-, filhandlings-, synkroniserings- og behandlingsstatus til autoriserte tenantbrukere;
- å vedlikeholde auditposter og driftslogger som dokumenterer hvilken Drive-handling som ble forespurt og fullført;
- feilsøking, sikkerhet, forebygging av misbruk, tvisteløsing og juridiske compliance-aktiviteter som er tillatt etter gjeldende policyer og tenantavtalen.

DynamicMail skal ikke selge Google Drive-data, bruke dem til annonsering eller retargeting, overføre dem til datameglere, bruke dem til overvåking eller bruke dem til å fastslå kredittverdighet eller låneberettigelse.

Bredt Drive-scope og narrowest-scope-merknad

Scopet `https://www.googleapis.com/auth/drive` er bredt fordi det kan gi tilgang til alle Drive-filer som er tilgjengelige for den tilkoblede kontoen. DynamicMail må behandle dette scopet som foreløpig til produkt- og compliance-review dokumenterer hvorfor smalere Drive-scopes ikke er tilstrekkelige for det implementerte workflowet.

For produksjonsbruk bør DynamicMail evaluere smalere Drive-scopes som `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` eller `drive.appfolder`. Hvis et smalere scope kan støtte den synlige funksjonen, må forespurt scope, samtykkeposter, OAuth-konfigurasjon, source asset, rendret asset og tester oppdateres før release.

Oppbevaring

DynamicMail oppbevarer Drive-avledede data bare så lenge det trengs for det synlige Drive-workflowet, tenantens innstillinger for dokumentoppbevaring, auditposter, sikkerhet, tvisteløsing eller juridisk compliance. OAuth-tokens og Drive-handlingsmetadata oppbevares bare så lenge de trengs for å drive den tilkoblede Drive-integrasjonen eller bevare påkrevde auditposter.

Drive-filinnhold, cachelagrede filer, metadata, OCR-tekst, uttrukne felter og avledede dokumentdata bør slettes eller anonymiseres når de ikke lenger trengs for det opplyste formålet, med mindre en juridisk, sikkerhetsmessig, auditmessig eller tenantoppbevaringsmessig forpliktelse krever fortsatt oppbevaring.

Sletting

En autorisert tenantbruker eller administrator kan be om sletting av cachelagrede Google-avledede data, importerte Drive-filer, uttrukket tekst og avledede dokumentposter. DynamicMail bør slette eller anonymisere de forespurte dataene når det er tillatt etter tenantens oppbevaringsinnstillinger og gjeldende rett.

Sletting av importerte DynamicMail-poster sletter ikke nødvendigvis den opprinnelige filen fra Google Drive. DynamicMail bør bare endre, flytte, legge i papirkurven eller slette opprinnelige Drive-filer når en autorisert bruker uttrykkelig ber om den Drive-handlingen gjennom et synlig produktworkflow, og handlingen er tillatt etter tenantpolicy og gjeldende rett.

Tilbakekalling og frakobling

Tenanten kan koble fra Google Drive i DynamicMail. Etter frakobling eller lokal tilbakekalling av samtykke må DynamicMail slutte å bruke lagrede OAuth-tokens for Google Drive og må slutte å lese, skrive, laste ned, laste opp, endre eller slette flere Drive-filer fra den tilkoblede kontoen.

Eieren av Google-kontoen kan også tilbakekalle appens autorisasjon i Google-kontoinnstillingene. Hvis Google-autorisasjonen tilbakekalles, må DynamicMail stoppe Drive API-tilgang når tokenoppdatering eller API-kall feiler, og tilkoblingen bør vises som frakoblet eller som krevende ny tilkobling.

Lokal tilbakekalling fjerner ikke automatisk allerede importerte DynamicMail-dokumenter. Disse postene håndteres etter reglene for sletting og oppbevaring ovenfor.

AI, OCR og uttrekk

DynamicMail kan bruke OCR, parsing, klassifisering, sammendrag og annen AI-støttet behandling av Drive-filinnhold og metadata bare for å levere eller forbedre det synlige Drive-dokumentworkflowet for tenanten. Drive-data og avledede data skal ikke brukes til å opprette, trene eller forbedre en generell maskinlærings- eller AI-modell utenfor funksjonen som tenanten har bedt om.

AI-støttede resultater kan være feil. DynamicMail bør presentere uttrukne data som workflow-output som autoriserte brukere kan gjennomgå, rette, godkjenne, avvise eller slette i henhold til produktflyten.

Support og menneskelig tilgang

DynamicMail-personell, kontraktører eller underdatabehandlere bør ikke lese spesifikke Drive-filer, uttrukket tekst, filmetadata eller avledede Drive-data med mindre ett av disse vilkårene gjelder:

- brukeren har uttrykkelig bedt om support som krever tilgang til spesifikke data;
- tilgangen er nødvendig for sikkerhetsundersøkelse, forebygging av misbruk eller incident response;
- tilgangen er nødvendig for å overholde rett, juridisk prosess eller en bindende tenantinstruks;
- dataene er aggregerte eller anonymiserte for intern drift, og ingen spesifikk brukers Drive-innhold er lesbart.

Supporttilgang bør være basert på minste nødvendige rettigheter, være tidsbegrenset der det er praktisk mulig og logges for audit.

Det er lokalisert implementerings- og reviewmateriale, ikke endelig juridisk rådgivning. Det må ikke presenteres som om det har Google-godkjenning, godkjenning fra ekstern juridisk rådgiver eller produksjonsklar restricted-scope-clearance uten separat reviewdokumentasjon.

Referanser

- 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