DYNAMICMAIL GOOGLE WORKSPACE TERMS

Vilkår for Gmail Readonly-dataadgang

Disse vilkår forklarer den Gmail inbound-adgang, som DynamicMail anmoder om, når en autoriseret tenantbruger eller administrator forbinder Gmail inbound-dokumentindtagelse til tenantens dokumentworkflows.

Google Sign-In-identitetsscopes som `openid`, `email` og `profile` er adskilt fra dette Gmail-dataadgangssamtykke. Login med Google betyder ikke, at Gmail inbound-adgang er accepteret.

Anmodet scope

DynamicMail anmoder kun om `https://www.googleapis.com/auth/gmail.readonly`, når en autoriseret tenantbruger eller administrator forbinder Gmail inbound-dokumentindtagelse. Dette Gmail-scope giver DynamicMail mulighed for at se Gmail-meddelelser og indstillinger for den forbundne Google-konto. DynamicMail bruger scopet til skrivebeskyttet inbound-behandling og bruger det ikke til at sende, ændre, slette, arkivere, etikettere eller flytte Gmail-meddelelser.

DynamicMail må ikke anmode om eller behandle Gmail-data, der ikke er relateret til den synlige Gmail inbound-dokumentindtagelsesfunktion.

Data, som DynamicMail kan tilgå

Når Gmail inbound er forbundet, kan DynamicMail tilgå de Gmail-data, der er nødvendige for at finde og behandle indgående forretningsdokumenter, herunder:

- meddelelses-id'er, tråd-id'er, historik-id'er, labelreferencer og synkroniseringsmarkører;
- afsender, modtager, emne, dato, headere og andre meddelelsesmetadata;
- meddelelsesindhold og uddrag, der er nødvendige for at identificere dokumentkontekst;
- vedhæftede filer og inline-filer, der kan indeholde fakturaer, meddelelser, aftaler, kvitteringer eller andre tenantdokumenter;
- Gmail-indstillinger kun hvor Gmail API'en kræver dem for readonly-scopet eller kontoens synkroniseringsadfærd;
- afledte data oprettet fra Gmail-indhold, for eksempel parsede dokumentfelter, OCR-tekst, klassifikationslabels, udtræksresultater, opsummeringer, audit-hændelser og dokumentposter.

Hvorfor DynamicMail bruger Gmail-data

DynamicMail bruger Gmail readonly-data til at levere den Gmail inbound-kilde, som tenanten har valgt. De tilsigtede formål er:

- at registrere indgående meddelelser, der kan indeholde tenantens forretningsdokumenter;
- at importere vedhæftede filer eller meddelelsesindhold, som tenanten vælger at behandle;
- at udtrække, klassificere og route dokumenter ind i DynamicMail-workflows;
- at afstemme synkroniseringstilstand, så den samme meddelelse ikke importeres gentagne gange;
- at vise forbindelses-, synkroniserings- og behandlingsstatus til autoriserede tenantbrugere;
- fejlfinding, sikkerhed, audit og juridiske compliance-aktiviteter, der er tilladt efter de gældende politikker og tenantaftalen.

DynamicMail må ikke sælge Gmail-data, bruge dem til annoncering eller retargeting, overføre dem til datahandlere, bruge dem til overvågning eller bruge dem til at fastslå kreditværdighed eller berettigelse til lån.

Opbevaring

DynamicMail opbevarer kun Gmail-afledte data så længe, som det er nødvendigt for den synlige inbound-dokumentfunktion, tenantens dokumentopbevaringsindstillinger, auditposter, sikkerhed, tvisthåndtering eller juridisk compliance. OAuth-tokens og synkroniseringsmetadata opbevares kun så længe, som de er nødvendige for at drive den forbundne Gmail inbound-kilde eller bevare påkrævede auditposter.

Rå Gmail-meddelelsesindhold, vedhæftede filer og afledte dokumentdata bør slettes eller anonymiseres, når de ikke længere er nødvendige for det oplyste formål, medmindre en juridisk, sikkerhedsmæssig, auditmæssig eller tenantopbevaringsmæssig forpligtelse kræver fortsat opbevaring.

Sletning

En autoriseret tenantbruger eller administrator kan anmode om sletning af cachelagrede Google-afledte data, importerede vedhæftede filer, udtrukket tekst og afledte dokumentposter. DynamicMail bør slette eller anonymisere de anmodede data, når det er tilladt efter tenantens opbevaringsindstillinger og gældende ret.

Sletning af importerede DynamicMail-poster sletter ikke nødvendigvis den oprindelige e-mail eller vedhæftede fil fra Gmail, fordi Gmail readonly-scopet ikke giver DynamicMail tilladelse til at ændre eller slette Gmail-meddelelser.

Tilbagekaldelse og afbrydelse

Tenanten kan afbryde Gmail inbound i DynamicMail. Efter afbrydelse eller lokal tilbagekaldelse af samtykke må DynamicMail ikke længere bruge gemte OAuth-tokens til Gmail inbound og må ikke læse yderligere Gmail-meddelelser fra den forbundne konto.

Ejeren af Google-kontoen kan også tilbagekalde appens autorisation i Google-kontoindstillingerne. Hvis Google-autorisationen tilbagekaldes, skal DynamicMail stoppe Gmail API-adgang, når tokenopdatering eller API-kald fejler, og forbindelsen bør vises som afbrudt eller som krævende genforbindelse.

En lokal tilbagekaldelse fjerner ikke automatisk allerede importerede DynamicMail-dokumenter. Disse poster håndteres efter reglerne for sletning og opbevaring ovenfor.

AI, OCR og udtræk

DynamicMail kan bruge OCR, parsing, klassificering, opsummering og anden AI-understøttet behandling på Gmail-afledt meddelelsesindhold og vedhæftede filer kun for at levere eller forbedre det synlige inbound-dokumentworkflow for tenanten. Gmail-data og afledte data må ikke bruges til at oprette, træne eller forbedre en generel machine-learning- eller AI-model uden for den funktion, tenanten har anmodet om.

AI-understøttede resultater kan være forkerte. DynamicMail bør præsentere udtrukne data som workflow-output, som autoriserede brugere kan gennemgå, rette, godkende, afvise eller slette efter produktflowet.

Support og menneskelig adgang

DynamicMail-personale, kontrakttagere eller underdatabehandlere bør ikke læse specifikke Gmail-meddelelser, vedhæftede filer, udtrukket tekst eller afledte Gmail-data, medmindre en af disse betingelser gælder:

- brugeren har udtrykkeligt bedt om support, der kræver adgang til specifikke data;
- adgangen er nødvendig for sikkerhedsundersøgelse, misbrugsforebyggelse eller incident response;
- adgangen er nødvendig for at overholde ret, juridisk proces eller en bindende tenantinstruks;
- dataene er aggregerede eller anonymiserede til interne operationer, og ingen specifik brugers Gmail-indhold er læsbart.

Supportadgang bør være baseret på mindst mulige rettigheder, være tidsbegrænset hvor det er praktisk muligt og logges af hensyn til audit.

Det er lokaliseret implementerings- og reviewmateriale, ikke endelig juridisk rådgivning. Det må ikke præsenteres som om det bærer Google-godkendelse, ekstern counsel-godkendelse eller produktionsklar restricted-scope-clearance uden særskilt reviewdokumentation.

Referencer

- 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