

Vilkår for Google Drive-dataadgang

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

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

Anmodet scope

DynamicMail anmoder kun om `https://www.googleapis.com/auth/drive`, når en autoriseret tenantbruger eller administrator forbinder Google Drive til tenantens dokumentworkflows. Dette er et bredt restricted Drive-scope, som kan give DynamicMail mulighed for at se og administrere alle filer på den forbundne Google Drive-konto, herunder filer som brugeren ejer, filer delt med brugeren, mapper og shared-drive-indhold, der er tilgængeligt for kontoen.

DynamicMail skal kun bruge Drive-scopet til oplyste, synlige Drive-dokumentworkflows, som tenanten har valgt. DynamicMail bør ikke anmode om, gennemse, kopiere, downloade, ændre, slette eller på anden måde behandle Drive-data, der ikke er relateret til det synlige Drive-dokumentworkflow.

Data, som DynamicMail kan tilgå

Når Google Drive er forbundet, kan DynamicMail tilgå de Drive-data, der er nødvendige for at levere tenantens valgte workflow, herunder:

- fil-id'er, navne, MIME-typer, checksums, størrelse, tidsstempler, beskrivelser, labels, mappereferencer, overordnede mapper og andre filmetadata;
- mappemetadata, shared-drive-metadata og søge- eller listningsresultater, der er nødvendige for at finde tenantdokumenter;
- filindhold, previews, thumbnails, eksporter, downloads, uploads og genererede eller redigerede filpayloads;
- delings- og tilladelsesmetadata, når de er nødvendige for at vise eller fuldføre en synlig Drive-filhandling;
- kontooverordnede Drive-oversigtsoplysninger, der er nødvendige for at bekræfte den forbundne konto og forbindelsesstatus;
- gemte kopier eller cachelagrede udtræk af Drive-filer, der er importeret til DynamicMail;

- afledte data oprettet fra Drive-filer, for eksempel OCR-tekst, parsede dokumentfelter, klassifikationslabels, udtræksresultater, opsummeringer, audit-hændelser og dokumentposter.

Formål med brugen

DynamicMail bruger Google Drive-data til at levere Drive-dokumentworkflows valgt af tenanten. De tilsigtede formål er:

- at lade autoriserede brugere forbinde Drive som dokumentkilde eller dokumentdestination;
- at finde, liste, importere, downloade, eksportere, uploade eller opdatere tenantens forretningsdokumenter, som er valgt gennem produktflowet;
- at udtrække, klassificere og route Drive-dokumenter ind i DynamicMail-workflows;
- at vise forbindelses-, filhandlings-, synkroniserings- og behandlingsstatus til autoriserede tenantbrugere;
- at vedligeholde auditposter og driftslogs, der dokumenterer, hvilken Drive-handling der blev anmodet om og fuldført;
- fejlfinding, sikkerhed, misbrugsforebyggelse, tvisthåndtering og juridiske compliance-aktiviteter, der er tilladt efter de gældende politikker og tenantaftalen.

DynamicMail må ikke sælge Google Drive-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.

Bredt Drive-scope og narrowest-scope-bemærkning

Scopet <https://www.googleapis.com/auth/drive> er bredt, fordi det kan give adgang til alle Drive-filer, der er tilgængelige for den forbundne konto. DynamicMail skal behandle dette scope som foreløbigt, indtil produkt- og compliance-review dokumenterer, hvorfor smallere Drive-scopes ikke er tilstrækkelige for det implementerede workflow.

For produktionsbrug bør DynamicMail evaluere smallere Drive-scopes som `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` eller `drive.appfolder`. Hvis et smallere scope kan understøtte den synlige funktion, skal det anmodede scope, samtykkeposter, OAuth-konfiguration, source asset, renderet asset og tests opdateres før release.

Opbevaring

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

Drive-filindhold, cachelagrede filer, metadata, OCR-tekst, udtrukne felter 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 Drive-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 fil fra Google Drive. DynamicMail bør kun ændre, flytte, lægge i papirkurven eller slette oprindelige Drive-filer, når en autoriseret bruger udtrykkeligt anmoder om den Drive-handling gennem et synligt produktworkflow, og handlingen er tilladt efter tenantpolitik og gældende ret.

Tilbagekaldelse og afbrydelse

Tenanten kan afbryde Google Drive i DynamicMail. Efter afbrydelse eller lokal tilbagekaldelse af samtykke må DynamicMail ikke længere bruge gemte OAuth-tokens til Google Drive og må ikke længere læse, skrive, downloade, uploade, ændre eller slette yderligere Drive-filer fra den forbundne konto.

Ejeren af Google-kontoen kan også tilbagekalde appens autorisation i Google-kointodstillingerne. Hvis Google-autorisationen tilbagekaldes, skal DynamicMail stoppe Drive 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 Drive-filindhold og metadata kun for at levere eller forbedre det synlige Drive-dokumentworkflow for tenanten. Drive-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 Drive-filer, udtrukket tekst, filmetadata eller afledte Drive-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 Drive-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>.
- 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>