

Villkor för Google Drive-dataåtkomst

Dessa villkor förklarar den Google Drive-åtkomst som DynamicMail begär när en behörig tenantanvändare eller administratör ansluter Google Drive till tenantens dokumentflöden.

Google Sign-In-identitetssscopes som `openid`, `email` och `profile` är separata från detta samtycke till Google Drive-dataåtkomst. Inloggning med Google betyder inte att Google Drive-åtkomst har accepterats.

Begärt scope

DynamicMail begär endast `https://www.googleapis.com/auth/drive` när en behörig tenantanvändare eller administratör ansluter Google Drive till tenantens dokumentflöden. Detta är ett brett restricted Drive-scope som kan göra det möjligt för DynamicMail att visa och hantera alla filer i det anslutna Google Drive-kontot, inklusive filer som användaren äger, filer som delas med användaren, mappar och innehåll på delade enheter som är tillgängligt för kontot.

DynamicMail ska endast använda Drive-scopet för redovisade, synliga Drive-dokumentflöden som tenanten har valt. DynamicMail bör inte begära, bläddra i, kopiera, ladda ned, ändra, radera eller på annat sätt behandla Drive-data som inte är relaterade till det synliga Drive-dokumentflödet.

Data som DynamicMail kan få åtkomst till

När Google Drive är anslutet kan DynamicMail få åtkomst till de Drive-data som behövs för att leverera tenantens valda arbetsflöde, inklusive:

- fil-ID:n, namn, MIME-typer, checksummor, storlek, tidsstämplar, beskrivningar, etiketter, mapppreferenser, överordnade mappar och andra filmetadata;
- mappmetadata, metadata för delade enheter och sök- eller listningsresultat som behövs för att hitta tenantdokument;
- filinnehåll, förhandsvisningar, miniatyrbilder, exporter, nedladdningar, uppladdningar och genererade eller redigerade filpayloads;
- delnings- och behörighetsmetadata när de behövs för att visa eller slutföra en synlig Drive-filåtgärd;
- kontoövergripande Drive-sammanfattningsinformation som behövs för att bekräfta det anslutna kontot och anslutningsstatus;
- sparade kopior eller cachelagrade extrakt av Drive-filer som importerats till DynamicMail;

- härledda data som skapats från Drive-filer, till exempel OCR-text, tolkade dokumentfält, klassificeringsetiketter, extraktionsresultat, sammanfattningar, audit-händelser och dokumentposter.

Ändamål med användningen

DynamicMail använder Google Drive-data för att leverera Drive-dokumentflöden som tenanten har valt. De avsedda ändamålen är:

- att låta behöriga användare ansluta Drive som dokumentkälla eller dokumentdestination;
- att hitta, lista, importera, ladda ned, exportera, ladda upp eller uppdatera tenantens affärsdokument som valts genom produktflödet;
- att extrahera, klassificera och dirigera Drive-dokument till DynamicMail-arbetsflöden;
- att visa anslutnings-, filåtgärds-, synkroniserings- och behandlingsstatus för behöriga tenantanvändare;
- att underhålla auditposter och driftloggar som visar vilken Drive-åtgärd som begärdes och slutfördes;
- felsökning, säkerhet, förebyggande av missbruk, tvistlösning och juridiska compliance-aktiviteter som är tillåtna enligt tillämpliga policyer och tenantavtalet.

DynamicMail får inte sälja Google Drive-data, använda dem för annonsering eller retargeting, överföra dem till datamäklare, använda dem för övervakning eller använda dem för att fastställa kreditvärdighet eller berättigande till lån.

Brett Drive-scope och narrowest-scope-anmärkning

Scopet <https://www.googleapis.com/auth/drive> är brett eftersom det kan ge åtkomst till alla Drive-filer som är tillgängliga för det anslutna kontot. DynamicMail måste behandla detta scope som provisoriskt tills produkt- och compliance-granskning dokumenterar varför smalare Drive-scopes inte är tillräckliga för det implementerade arbetsflödet.

Före produktionsanvändning bör DynamicMail utvärdera smalare Drive-scopes som `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` eller `drive.appfolder`. Om ett smalare scope kan stödja den synliga funktionen måste begärt scope, samtyckesposter, OAuth-konfiguration, källasset, renderat asset och tester uppdateras före release.

Lagring

DynamicMail lagrar Drive-härledda data endast så länge det behövs för det synliga Drive-flödet, tenantens inställningar för dokumentlagring, auditposter, säkerhet, tvistlösning eller juridisk compliance. OAuth-token och Drive-åtgärdsmetadata lagras endast så länge de behövs för att driva den anslutna Drive-integrationen eller bevara krävda auditposter.

Drive-filinnehall, cachelagrade filer, metadata, OCR-text, extraherade fält och härledda dokumentdata bör raderas eller anonymiseras när de inte längre behövs för det angivna ändamålet, om inte en juridisk, säkerhets-, audit- eller tenantlagringsförpliktelse kräver fortsatt lagring.

Radering

En behörig tenantanvändare eller administratör kan begära radering av cachelagrade Google-härledda data, importerade Drive-filer, extraherad text och härledda dokumentposter. DynamicMail bör radera eller anonymisera de begärda uppgifterna när det är tillåtet enligt tenantens lagringsinställningar och tillämplig rätt.

Radering av importerade DynamicMail-poster raderar inte nödvändigtvis den ursprungliga filen från Google Drive. DynamicMail bör endast ändra, flytta, lägga i papperskorgen eller radera ursprungliga Drive-filer när en behörig användare uttryckligen begär den Drive-åtgärden genom ett synligt produktflöde och åtgärden är tillåten enligt tenantpolicy och tillämplig rätt.

Återkallelse och frånkoppling

Tenanten kan koppla från Google Drive i DynamicMail. Efter frånkoppling eller lokal återkallelse av samtycke får DynamicMail inte längre använda lagrade OAuth-token för Google Drive och får inte längre läsa, skriva, ladda ned, ladda upp, ändra eller radera ytterligare Drive-filer från det anslutna kontot.

Ägaren av Google-kontot kan också återkalla appens auktorisering i Google-kontoinställningarna. Om Google-auktoriseringen återkallas måste DynamicMail stoppa Drive API-åtkomst när tokenuppdatering eller API-anrop misslyckas, och anslutningen bör visas som frånkopplad eller som kräver återanslutning.

En lokal återkallelse tar inte automatiskt bort redan importerade DynamicMail-dokument. Dessa poster hanteras enligt reglerna för radering och lagring ovan.

AI, OCR och extraktion

DynamicMail kan använda OCR, parsning, klassificering, sammanfattning och annan AI-stödd behandling av Drive-filinnehall och metadata endast för att leverera eller förbättra det synliga Drive-dokumentarbetsflödet för tenanten. Drive-data och härledda data får inte användas för att skapa, träna eller förbättra en generell maskininlärnings- eller AI-modell utanför den funktion som tenanten har begärt.

AI-stödda resultat kan vara felaktiga. DynamicMail bör presentera extraherade data som arbetsflödesresultat som behöriga användare kan granska, rätta, godkänna, avvisa eller radera enligt produktflödet.

Support och mänsklig åtkomst

DynamicMail-personal, kontraktstagare eller underbiträden bör inte läsa specifika Drive-filer, extraherad text, filmetadata eller härledda Drive-data om inte ett av dessa villkor gäller:

- användaren har uttryckligen bett om support som kräver åtkomst till specifika data;
- åtkomsten är nödvändig för säkerhetsutredning, förebyggande av missbruk eller incidenthantering;
- åtkomsten är nödvändig för att följa lag, juridisk process eller en bindande tenantinstruktion;
- data är aggregerade eller anonymiserade för intern drift och ingen specifik användares Drive-innehåll är läsbart.

Supportåtkomst bör bygga på minsta möjliga behörighet, vara tidsbegränsad där det är praktiskt möjligt och loggas för audit.

Det är lokaliserat implementerings- och granskningsmaterial, inte slutlig juridisk rådgivning. Det får inte presenteras som om det har Google-godkännande, godkännande från extern juridisk rådgivare eller produktionsklar restricted-scope-clearance utan separat granskningsdokumentation.

Referenser

- 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>