

Google Drive datu piekļuves noteikumi

Šajos noteikumos ir paskaidrota Google Drive piekļuve, ko DynamicMail pieprasa, kad pilnvarots klienta organizācijas lietotājs vai administrators pievieno Google Drive klienta organizācijas dokumentu darbplūsmām.

Google Sign-In identitātes tvērumi, piemēram, openid, email un profile, ir nošķirti no šīs piekrišanas Google Drive datu piekļuvei. Pierakstīšanās ar Google nenožīmē Google Drive piekļuves pieņemšanu.

Pieprasītais tvērums

DynamicMail pieprasa <https://www.googleapis.com/auth/drive> tikai tad, kad pilnvarots klienta organizācijas lietotājs vai administrators pievieno Google Drive klienta organizācijas dokumentu darbplūsmām. Tas ir plašs ierobežots Drive tvērums, kas var ļaut DynamicMail skatīt un pārvaldīt visus pievienotā Google Drive konta failus, tostarp lietotājam piederošus failus, ar lietotāju kopīgotus failus, mapes un šim kontam pieejamo kopīgo disku saturu.

DynamicMail jāizmanto Drive tvērums tikai atklātām, redzamām Drive dokumentu darbplūsmām, ko izvēlējusies klienta organizācija. DynamicMail nedrīkst pieprasīt, pārlūkot, kopēt, lejupielādēt, mainīt, dzēst vai citādi apstrādāt Drive datus, kas nepieder redzamai Drive dokumentu darbplūsmai.

Dati, kuriem DynamicMail var piekļūt

Kad Google Drive ir pievienots, DynamicMail var piekļūt Drive datiem, kas nepieciešami izvēlētās klienta organizācijas darbplūsmas nodrošināšanai, tostarp:

- failu ID, nosaukumiem, MIME tiem, kontrolsummām, izmēram, laika zīmogiem, aprakstiem, etiķetēm, mapju atsaucēm, vecākmapēm un citiem failu metadatiem;
- mapju metadatiem, kopīgo disku metadatiem un meklēšanas vai sarakstu rezultātiem, kas nepieciešami klienta organizācijas dokumentu atrašanai;
- failu saturam, priekšskatījumiem, sīktēliem, eksportiem, lejupielādēm, augšupielādēm un izveidotiem vai rediģētiem failu kopumiem;
- kopīgošanas un atļauju metadatiem, kad tie nepieciešami redzamas Drive faila darbības parādīšanai vai pabeigšanai;
- konta līmeņa Drive kopsavilkuma informācijai, kas nepieciešama pievienotā konta un savienojuma statusa apstiprināšanai;
- saglabātām Drive failu kopijām vai kešotiem izvilkumiem, kas importēti DynamicMail;

- no Drive failiem izveidotiem atvasinātiem datiem, piemēram, OCR tekstam, parsētiem dokumentu laukiem, klasifikācijas etiķetēm, izgūšanas rezultātiem, kopsavilkumiem, audita notikumiem un dokumentu ierakstiem.

Izmantošanas nolūks

DynamicMail izmanto Google Drive datus, lai nodrošinātu klienta organizācijas izvēlētās Drive dokumentu darbplūsmas. Paredzētie nolūki ir:

- ļaut pilnvarotiem lietotājiem pievienot Drive kā dokumentu avotu vai galamērķi;
- atrast, uzskaitīt, importēt, lejupielādēt, eksportēt, augšupielādēt vai atjaunināt klienta organizācijas biznesa dokumentus, kas izvēlēti produkta plūsmā;
- izgūt un klasificēt Drive dokumentus un novirzīt tos DynamicMail darbplūsmās;
- rādīt savienojuma, failu darbību, sinhronizācijas un apstrādes statusu pilnvarotiem klienta organizācijas lietotājiem;
- uzturēt audita ierakstus un operatīvos žurnālus, kas apliecina, kāda Drive darbība tika pieprasīta un pabeigta;
- veikt problēmu novēršanas, drošības, ļaunprātīgas izmantošanas novēršanas, strīdu izskatīšanas un tiesiskās atbilstības darbības, ko atļauj piemērojamās politikas un klienta organizācijas līgums.

DynamicMail nedrīkst pārdot Google Drive datus, izmantot tos reklāmai vai atkārtotai mērķēšanai, nodot tos datu brokeriem, izmantot tos uzraudzībai vai izmantot kredītpējas vai tiesību uz aizdevumu noteikšanai.

Plašais Drive tvērums un piezīme par šaurāko tvērumu

Tvērums <https://www.googleapis.com/auth/drive> ir plašs, jo tas var ļaut piekļūt visiem Drive failiem, kas pieejami pievienotajam kontam. DynamicMail jāuzskata šis tvērums par provizorisku, līdz produkta un atbilstības pārskatīšana dokumentē, kāpēc šaurāki Drive tvērumi nav pietiekami īstenotajai darbplūsmai.

Pirms izmantošanas ražošanā DynamicMail jāizvērtē šaurāki Drive tvērumi, piemēram, `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` vai `drive.appfolder`. Ja šaurāks tvērums var atbalstīt redzamo funkciju, pirms izlaišanas jāatjaunina pieprasītais tvērums, piekrišanas ieraksti, OAuth konfigurācija, avota resurss, ģenerētais resurss un testi.

Glabāšana

DynamicMail glabā no Drive iegūtos datus tikai tik ilgi, cik tas nepieciešams redzamajai Drive darbplūsmai, klienta organizācijas dokumentu glabāšanas iestatījumiem, audita ierakstiem, drošībai, strīdu izskatīšanai vai tiesiskajai atbilstībai. OAuth piekļuves marķieri un Drive darbību metadati tiek glabāti tikai tik ilgi, cik tie nepieciešami pievienotās Drive integrācijas darbībai vai nepieciešamo audita ierakstu saglabāšanai.

Drive failu saturs, kešotie faili, metadati, OCR teksts, izgūtie lauki un atvasinātie dokumentu dati ir jādzēš vai jāanonimizē, kad tie vairs nav nepieciešami atklātajam nolūkam, izņemot gadījumus, kad juridisks, drošības, audita vai klienta organizācijas glabāšanas pienākums prasa turpināt to glabāšanu.

Dzēšana

Pilnvarots klienta organizācijas lietotājs vai administrators var pieprasīt dzēst no Google iegūtos kešotos datus, importētos Drive failus, izgūto tekstu un atvasinātos dokumentu ierakstus. DynamicMail jādzēš vai jāanonimizē pieprasītie dati, kad to atļauj klienta organizācijas glabāšanas iestatījumi un piemērojamie tiesību akti.

Importēto DynamicMail ierakstu dzēšana ne vienmēr dzēš sākotnējo failu no Google Drive. DynamicMail drīkst mainīt, pārvietot, pārvietot uz atkritni vai dzēst sākotnējos Drive failus tikai tad, kad pilnvarots lietotājs skaidri pieprasa šādu Drive darbību redzamā produkta darbplūsmā un darbību atļauj klienta organizācijas politika un piemērojamie tiesību akti.

Atsauksana un atvienošana

Klienta organizācija var atvienot Google Drive DynamicMail sistēmā. Pēc atvienošanas vai vietējās piekrišanas atsauksanas DynamicMail vairs nedrīkst izmantot saglabātos OAuth piekļuves marķierus Google Drive un vairs nedrīkst lasīt, rakstīt, lejupielādēt, augšupielādēt, mainīt vai dzēst papildu Drive failus no pievienotā konta.

Google konta īpašnieks var arī atsaukt lietotnes autorizāciju Google konta iestatījumos. Ja Google autorizācija tiek atsaukta, DynamicMail jāpārtrauc Drive API piekļuve, kad piekļuves marķiera atsvaizdināšana vai API pieprasījumi neizdodas, un savienojums jārāda kā atvienots vai tāds, kam nepieciešama atkārtota pievienošana.

Vietējā atsauksana automātiski nenoņem jau importētos DynamicMail dokumentus. Šie ieraksti tiek apstrādāti saskaņā ar iepriekš norādītajiem dzēšanas un glabāšanas noteikumiem.

MI, OCR un izgūšana

DynamicMail var izmantot OCR, parsēšanu, klasifikāciju, kopsavilkumu veidošanu un citu MI atbalstītu apstrādi Drive failu saturam un metadatiem tikai tādēļ, lai nodrošinātu vai uzlabotu klienta organizācijai redzamo Drive dokumentu darbplūsmu. Drive datus un atvasinātos datus nedrīkst izmantot vispārīga nolūka mašīnmācīšanās vai MI modeļa izveidei, apmācīšanai vai uzlabošanai ārpus klienta organizācijas pieprasītās funkcijas.

MI atbalstīti rezultāti var būt kļūdaini. DynamicMail jāparāda izgūtie dati kā darbplūsmas rezultāts, ko pilnvaroti lietotāji var pārskatīt, labot, apstiprināt, noraidīt vai dzēst atbilstoši produkta plūsmai.

Atbalsts un cilvēka piekļuve

DynamicMail darbinieki, darbuņēmēji vai apakšapstrādātāji nedrīkst lasīt konkrētus Drive failus, izgūto tekstu, failu metadatus vai atvasinātos Drive datus, ja vien nav spēkā viens no šiem nosacījumiem:

- lietotājs ir skaidri lūdzis atbalstu, kam nepieciešama piekļuve konkrētiem datiem;
- piekļuve ir nepieciešama drošības izmeklēšanai, ļaunprātīgas izmantošanas novēršanai vai incidentu pārvaldībai;
- piekļuve ir nepieciešama, lai ievērotu tiesību aktus, juridisku procesu vai saistošu klienta organizācijas norādījumu;
- dati ir agregēti vai anonimizēti iekšējām darbībām, un konkrēta lietotāja Drive saturs nav salasāms.

Atbalsta piekļuvei jābalstās uz mazāko nepieciešamo tiesību principu, tai jābūt ierobežotai laikā, kad tas ir praktiski iespējams, un reģistrētai auditam.

Tas ir lokalizēts ieviešanas un pārskatīšanas teksts, nevis galīga juridiska konsultācija. To nedrīkst pasniegt tā, it kā tam būtu Google apstiprinājums, ārēja jurista apstiprinājums vai ražošanas restricted-scope pielaide bez atsevišķiem pārskatīšanas pierādījumiem.

Atsauces

- 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>