

Podmienky prístupu k dátam Google Drive

Tieto podmienky vysvetľujú prístup ku Google Drive, ktorý DynamicMail požaduje, keď oprávnený používateľ alebo správca tenantu pripojí Google Drive pre pracovné postupy s dokumentmi tenantu.

Identitné rozsahy Google Sign-In, ako openid, email a profile, sú oddelené od tohto súhlasu s prístupom k dátam Google Drive. Prihlásenie cez Google neznamená prijatie prístupu ku Google Drive.

Požadovaný rozsah

DynamicMail požaduje <https://www.googleapis.com/auth/drive> iba vtedy, keď oprávnený používateľ alebo správca tenantu pripojí Google Drive pre pracovné postupy s dokumentmi tenantu. Ide o široký obmedzený rozsah Drive, ktorý môže DynamicMail umožniť zobrazovať a spravovať všetky súbory v pripojenom účte Google Drive vrátane súborov vlastnených používateľom, súborov zdieľaných s používateľom, priečinkov a obsahu zdieľaných diskov dostupného pre tento účet.

DynamicMail musí používať rozsah Drive iba pre zverejnené, viditeľné pracovné postupy s dokumentmi v Drive, ktoré tenant vybral. DynamicMail by nemal požadovať, prechádzať, kopírovať, sťahovať, upravovať, mazať ani inak spracúvať dáta Drive, ktoré nesúvisia s viditeľným pracovným postupom s dokumentmi v Drive.

Dáta, ku ktorým môže mať DynamicMail prístup

Keď je Google Drive pripojený, DynamicMail môže mať prístup k dátam Drive potrebným na poskytnutie vybraného pracovného postupu tenantu vrátane:

- ID súborov, názvov, typov MIME, kontrolných súčtov, veľkosti, časových pečiatok, opisov, štítkov, odkazov na priečinky, nadradených priečinkov a ďalších metadát súborov;
- metadát priečinkov, metadát zdieľaných diskov a výsledkov vyhľadávania alebo výpisov potrebných na nájdenie dokumentov tenantu;
- obsahu súborov, náhľadov, miniatúr, exportov, sťahovaní, nahrávaní a generovaných alebo upravovaných dát súborov;
- metadát zdieľania a oprávnení, keď sú potrebné na zobrazenie alebo dokončenie viditeľnej operácie so súborom v Drive;
- súhrnných informácií na úrovni účtu Drive potrebných na potvrdenie pripojeného účtu a stavu pripojenia;

- uložených kópií alebo kešovaných extraktov súborov Drive importovaných do DynamicMail;
- odvodených dát vytvorených zo súborov Drive, ako sú text OCR, parsované polia dokumentov, klasifikačné štítky, výsledky extrakcie, súhrny, auditné udalosti a záznamy dokumentov.

Účel použitia

DynamicMail používa dáta Google Drive na poskytovanie pracovných postupov s dokumentmi v Drive, ktoré tenant vybral. Zamýšľané účely sú:

- umožniť oprávneným používateľom pripojiť Drive ako zdroj alebo cieľ dokumentov;
- vyhľadávať, vypisovať, importovať, sťahovať, exportovať, nahrávať alebo aktualizovať firemné dokumenty tenantu vybrané v produktovom toku;
- extrahovať, klasifikovať a smerovať dokumenty Drive do pracovných postupov DynamicMail;
- zobrazovať stav pripojenia, súborových operácií, synchronizácie a spracovania oprávneným používateľom tenantu;
- udržiavať auditné záznamy a prevádzkové protokoly, ktoré preukazujú, aká operácia v Drive bola požadovaná a dokončená;
- vykonávať riešenie problémov, bezpečnosť, prevenciu zneužitia, riešenie sporov a činnosti právneho súladu povolené príslušnými zásadami a zmluvou s tenantom.

DynamicMail nesmie predávať dáta z Google Drive, používať ich na reklamu alebo retargeting, prenášať ich sprostredkovateľom dát, používať ich na sledovanie ani ich používať na určovanie bonity alebo oprávnenosti na poskytnutie úveru.

Široký rozsah Drive a poznámka k najužšiemu rozsahu

Rozsah <https://www.googleapis.com/auth/drive> je široký, pretože môže umožniť prístup ku všetkým súborom v Drive dostupným pre pripojený účet. DynamicMail musí tento rozsah považovať za provizórny, kým produktové a compliance posúdenie nezdokumentuje, prečo užšie rozsahy Drive nie sú pre implementovaný pracovný postup dostatočné.

Pred produkčným použitím by DynamicMail mal vyhodnotiť užšie rozsahy Drive, ako `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` alebo `drive.appfolder`. Ak užší rozsah môže podporovať viditeľnú funkciu, pred vydaním sa musí aktualizovať požadovaný rozsah, záznamy súhlasu, konfigurácia OAuth, zdrojový asset, vykreslený asset a testy.

Uchovávanie

DynamicMail uchováva dáta odvodené z Drive iba tak dlho, ako je potrebné pre viditeľný pracovný postup v Drive, nastavenia uchovávanie dokumentov tenantu, auditné záznamy, bezpečnosť, riešenie sporov alebo právny súlad. OAuth tokeny a metadáta

operácií Drive sa uchovávali iba tak dlho, ako sú potrebné na prevádzku pripojenej integrácie Drive alebo na zachovanie povinných auditných záznamov.

Obsah súborov Drive, kešované súbory, metadáta, text OCR, extrahované polia a odvodené dáta dokumentov by sa mali odstrániť alebo anonymizovať, keď už nie sú potrebné na zverejnený účel, pokiaľ právna, bezpečnostná, auditná alebo tenantom určená povinnosť uchovávania nevyžaduje ďalšie uchovanie.

Odstránenie

Oprávnený používateľ alebo správca tenantu môže požiadať o odstránenie kešovaných dát odvodených od Google, importovaných súborov Drive, extrahovaného textu a odvodených záznamov dokumentov. DynamicMail by mal požadované dáta odstrániť alebo anonymizovať, ak to umožňujú nastavenia uchovávania tenantu a príslušné právo.

Odstránenie importovaných záznamov DynamicMail nemusí nevyhnutne odstrániť pôvodný súbor z Google Drive. DynamicMail by mal pôvodné súbory Drive upravovať, presúvať, presúvať do koša alebo mazať iba vtedy, keď oprávnený používateľ výslovne požiada o takúto akciu Drive prostredníctvom viditeľného produktového pracovného postupu a akcia je povolená zásadami tenantu a príslušným právom.

Odvolanie a odpojenie

Tenant môže v DynamicMail odpojiť Google Drive. Po odpojení alebo lokálnom odvolaní súhlasu musí DynamicMail prestať používať uložené OAuth tokeny pre Google Drive a musí prestať čítať, zapisovať, sťahovať, nahrávať, upravovať alebo mazať ďalšie súbory Drive z pripojeného účtu.

Vlastník účtu Google môže tiež odvolať autorizáciu aplikácie v nastaveniach účtu Google. Ak je autorizácia Google odvolaná, DynamicMail musí zastaviť prístup k Drive API, keď zlyhá obnovenie tokenu alebo volania API, a pripojenie by sa malo zobrazovať ako odpojené alebo vyžadujúce opätovné pripojenie.

Lokálne odvolanie automaticky neodstráni už importované dokumenty DynamicMail. Tieto záznamy sa riadia vyššie uvedenými pravidlami pre odstránenie a uchovávanie.

AI, OCR a extrakcia

DynamicMail môže používať OCR, parsovanie, klasifikáciu, sumarizáciu a iné spracovanie podporované AI nad obsahom súborov a metadátami odvodenými z Drive iba na poskytnutie alebo zlepšenie viditeľného pracovného postupu s dokumentmi v Drive pre tenant. Dáta z Drive a odvodené dáta sa nesmú použiť na vytváranie, trénovanie alebo zlepšovanie všeobecného modelu strojového učenia alebo AI mimo funkcie vyžadanej tenantom.

Výsledky podporované AI môžu byť chybné. DynamicMail by mal extrahované dáta prezentovať ako výstup pracovného postupu, ktorý môžu oprávnení používatelia podľa

produktového toku kontrolovať, opravovať, schvaľovať, odmietať alebo mazať.

Prístup podpory a ľudský prístup

Pracovníci, dodávatelia alebo subdodávatelia DynamicMail by nemali čítať konkrétne súbory Drive, extrahovaný text, metadáta súborov ani odvodené dáta Drive, pokiaľ nie je splnená jedna z týchto podmienok:

- používateľ výslovne požiadal o podporu, ktorá vyžaduje prístup ku konkrétnym dátam;
- prístup je nevyhnutný na bezpečnostné vyšetrovanie, prevenciu zneužitia alebo reakciu na incident;
- prístup je nevyhnutný na splnenie práva, právneho procesu alebo záväzného pokynu tenantu;
- dáta sú agregované alebo anonymizované pre internú prevádzku a obsah Drive konkrétného používateľa nie je čitateľný.

Prístup podpory by mal byť založený na princípe najmenších oprávnení, časovo obmedzený tam, kde je to praktické, a mal by byť protokolovaný pre auditovateľnosť.

Stav posúdenia

Je to implementačný a lokalizačný materiál, nie konečná právna rada ani miestne právne poradenstvo. Bez samostatného dôkazu o posúdení nesmie byť prezentovaný ako nesúci schválenie spoločnosťou Google, schválenie externým právnym poradcom alebo produkčné povolenie pre obmedzený rozsah.

Referencie

- 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>