

Podmínky přístupu k datům Google Drive

Tyto podmínky vysvětlují přístup ke Google Drive, který DynamicMail požaduje, když oprávněný uživatel nebo správce tenantu připojí Google Drive pro pracovní postupy s dokumenty tenantu.

Identitní rozsahy Google Sign-In, jako openid, email a profile, jsou oddělené od tohoto souhlasu s přístupem k datům Google Drive. Přihlášení přes Google neznamená přijetí přístupu ke Google Drive.

Požadovaný rozsah

DynamicMail požaduje <https://www.googleapis.com/auth/drive> pouze tehdy, když oprávněný uživatel nebo správce tenantu připojí Google Drive pro pracovní postupy s dokumenty tenantu. Jde o široký omezený rozsah Drive, který může DynamicMail umožnit zobrazovat a spravovat všechny soubory v připojeném účtu Google Drive, včetně souborů vlastněných uživatelem, souborů sdílených s uživatelem, složek a obsahu sdílených disků dostupného pro tento účet.

DynamicMail musí používat rozsah Drive pouze pro zveřejněné, viditelné pracovní postupy s dokumenty v Drive, které tenant vybral. DynamicMail by neměl požadovat, procházet, kopírovat, stahovat, upravovat, mazat ani jinak zpracovávat data Drive, která nesouvisí s viditelným pracovním postupem s dokumenty v Drive.

Data, ke kterým může mít DynamicMail přístup

Když je Google Drive připojen, DynamicMail může mít přístup k datům Drive potřebným k poskytnutí vybraného pracovního postupu tenantu, včetně:

- ID souborů, názvů, typů MIME, kontrolních součtů, velikosti, časových razítek, popisů, štítků, odkazů na složky, nadřazených složek a dalších metadat souborů;
- metadat složek, metadat sdílených disků a výsledků vyhledávání nebo výpisů potřebných k nalezení dokumentů tenantu;
- obsahu souborů, náhledů, miniatur, exportů, stahování, nahrávání a generovaných nebo upravovaných dat souborů;
- metadat sdílení a oprávnění, pokud jsou potřeba k zobrazení nebo dokončení viditelné operace se souborem v Drive;
- souhrnných informací na úrovni účtu Drive potřebných k potvrzení připojeného účtu a stavu připojení;

- uložených kopií nebo kešovaných extraktů souborů Drive importovaných do DynamicMail;
- odvozených dat vytvořených ze souborů Drive, jako je text OCR, parsovaná pole dokumentů, klasifikační štítky, výsledky extrakce, souhrny, auditní události a záznamy dokumentů.

Účel použití

DynamicMail používá data Google Drive k poskytování pracovních postupů s dokumenty v Drive, které tenant vybral. Zamýšlené účely jsou:

- umožnit oprávněným uživatelům připojit Drive jako zdroj nebo cíl dokumentů;
- vyhledávat, vypisovat, importovat, stahovat, exportovat, nahrávat nebo aktualizovat firemní dokumenty tenantu vybrané v produktovém toku;
- extrahovat, klasifikovat a směřovat dokumenty Drive do pracovních postupů DynamicMail;
- zobrazovat stav připojení, souborových operací, synchronizace a zpracování oprávněným uživatelům tenantu;
- udržovat auditní záznamy a provozní protokoly, které prokazují, jaká operace v Drive byla požadována a dokončena;
- provádět řešení potíží, bezpečnost, prevenci zneužití, řešení sporů a činnosti právního souladu dovolené příslušnými pravidly a smlouvou s tenantem.

DynamicMail nesmí prodávat data z Google Drive, používat je pro reklamu nebo retargeting, převádět je zprostředkovatelům dat, používat je ke sledování ani je používat k určování bonity nebo způsobilosti k poskytnutí úvěru.

Široký rozsah Drive a poznámka k nejužšímu rozsahu

Rozsah <https://www.googleapis.com/auth/drive> je široký, protože může umožnit přístup ke všem souborům v Drive dostupným pro připojený účet. DynamicMail musí tento rozsah považovat za provizorní, dokud produktové a compliance posouzení nezdokumentuje, proč užší rozsahy Drive nejsou pro implementovaný pracovní postup dostatečné.

Před produkčním použitím by DynamicMail měl vyhodnotit užší rozsahy Drive, jako `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` nebo `drive.appfolder`. Pokud užší rozsah může podporovat viditelnou funkci, musí být před vydáním aktualizován požadovaný rozsah, záznamy souhlasu, konfigurace OAuth, zdrojový asset, vykreslený asset a testy.

Uchovávání

DynamicMail uchovává data odvozená z Drive pouze tak dlouho, jak je potřeba pro viditelný pracovní postup v Drive, nastavení uchovávání dokumentů tenantu, auditní záznamy, bezpečnost, řešení sporů nebo právní soulad. OAuth tokeny a metadata

operací Drive jsou uchovávány pouze tak dlouho, jak jsou potřeba k provozu připojené integrace Drive nebo k zachování povinných auditních záznamů.

Obsah souborů Drive, kešované soubory, metadata, text OCR, extrahovaná pole a odvozená data dokumentů by měly být odstraněny nebo anonymizovány, jakmile již nejsou potřeba pro zveřejněný účel, pokud právní, bezpečnostní, auditní nebo tenantem určená povinnost uchovávání nevyžaduje další uchování.

Odstranění

Oprávněný uživatel nebo správce tenantu může požádat o odstranění kešovaných dat odvozených z Google, importovaných souborů Drive, extrahovaného textu a odvozených záznamů dokumentů. DynamicMail by měl požadovaná data odstranit nebo anonymizovat, pokud to dovolují nastavení uchovávání tenantu a příslušné právo.

Odstranění importovaných záznamů DynamicMail nutně neodstraní původní soubor z Google Drive. DynamicMail by měl původní soubory Drive upravovat, přesouvat, přesouvat do koše nebo mazat pouze tehdy, když oprávněný uživatel takovou akci Drive výslovně požádá prostřednictvím viditelného produktového pracovního postupu a akce je dovolena pravidly tenantu a příslušným právem.

Odvolání a odpojení

Tenant může v DynamicMail odpojit Google Drive. Po odpojení nebo lokálním odvolání souhlasu musí DynamicMail přestat používat uložené OAuth tokeny pro Google Drive a musí přestat číst, zapisovat, stahovat, nahrávat, upravovat nebo mazat další soubory Drive z připojeného účtu.

Vlastník účtu Google může také odvolat autorizaci aplikace v nastaveních účtu Google. Pokud je autorizace Google odvolána, DynamicMail musí zastavit přístup k Drive API, když se nepodaří obnovení tokenu nebo volání API, a připojení by mělo být zobrazeno jako odpojené nebo vyžadující opětovné připojení.

Lokální odvolání automaticky neodstraní již importované dokumenty DynamicMail. Tyto záznamy se řídí výše uvedenými pravidly pro odstranění a uchovávání.

AI, OCR a extrakce

DynamicMail může používat OCR, parsování, klasifikaci, sumarizaci a jiné zpracování podporované AI nad obsahem souborů a metadaty odvozenými z Drive pouze k poskytnutí nebo zlepšení viditelného pracovního postupu s dokumenty v Drive pro tenant. Data z Drive a odvozená data nesmí být použita k vytváření, trénování nebo zlepšování obecného modelu strojového učení nebo AI mimo funkci vyžádanou tenantem.

Výsledky podporované AI mohou být chybné. DynamicMail by měl extrahovaná data prezentovat jako výstup pracovního postupu, který mohou oprávnění uživatelé podle

produktového toku kontrolovat, opravovat, schvalovat, odmítat nebo mazat.

Přístup podpory a lidský přístup

Pracovníci, dodavatelé nebo subdodavatelé DynamicMail by neměli číst konkrétní soubory Drive, extrahovaný text, metadata souborů ani odvozená data Drive, pokud není splněna jedna z těchto podmínek:

- uživatel výslovně požádal o podporu, která vyžaduje přístup ke konkrétním datům;
- přístup je nezbytný pro bezpečnostní vyšetřování, prevenci zneužití nebo reakci na incident;
- přístup je nezbytný ke splnění práva, právního procesu nebo závazného pokynu tenantu;
- data jsou agregovaná nebo anonymizovaná pro interní provoz a obsah Drive konkrétního uživatele není čitelný.

Přístup podpory by měl být založen na principu nejmenších oprávnění, pokud je to praktické časově omezený, a měl by být protokolován pro auditovatelnost.

Stav posouzení

Je to implementační a lokalizační materiál, není konečnou právní radou ani místním právním poradenstvím. Bez samostatného důkazu o posouzení nesmí být prezentován jako nesoucí schválení společností Google, schválení externím právním poradcem nebo produkční povolení pro omezený rozsah.

Reference

- 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>