

Google Drive डेटा एक्सेस शर्तें

यह दस्तावेज़ केवल Google Drive को कवर करता है। इसका उपयोग उसी Google Workspace asset family की Gmail रीड-ओनली शर्तों के साथ किया जाना है।

स्कोप

DynamicMail <https://www.googleapis.com/auth/drive> केवल तब मांगता है जब ग्राहक संगठन का कोई अधिकृत उपयोगकर्ता या प्रशासक ग्राहक संगठन के दस्तावेज़ workflows के लिए Google Drive को कनेक्ट करता है। यह एक broad restricted Drive scope है जो DynamicMail को connected Google Drive account में उपलब्ध सभी files को देखने और manage करने की अनुमति दे सकता है, जिनमें user-owned files, user के साथ shared files, folders और उस account को उपलब्ध shared-drive content शामिल हैं।

DynamicMail को Drive scope का उपयोग केवल उन disclosed, visible Drive document workflows के लिए करना होगा जिन्हें ग्राहक संगठन चुनता है। Google Sign-In identity scopes जैसे openid, email, और profile इस Drive data-access consent से अलग हैं। Google से sign in करने का अर्थ Google Drive access स्वीकार करना नहीं है।

DynamicMail किन डेटा तक पहुंच सकता है

जब Google Drive कनेक्ट होता है, DynamicMail चुने गए ग्राहक संगठन workflow को उपलब्ध कराने के लिए आवश्यक Drive data तक पहुंच सकता है, जिनमें शामिल हैं:

- file IDs, names, MIME types, checksums, size, timestamps, descriptions, labels, folder references, parent folders और अन्य file metadata;
- tenant documents खोजने के लिए आवश्यक folder metadata, shared-drive metadata और search/listing results;
- file content, previews, thumbnails, exports, downloads, uploads और generated या edited file payloads;
- visible Drive file operation दिखाने या पूरा करने के लिए आवश्यक sharing और permission metadata;
- connected account और connection status की पुष्टि करने के लिए आवश्यक account-level Drive summary information;
- DynamicMail में imported Drive files की stored copies या cached extracts;
- Drive files से बना derived data, जैसे OCR text, parsed document fields, classification labels, extraction results, summaries, audit events और document records।

DynamicMail को ऐसे Drive data का अनुरोध, browse, copy, download, modify, delete या अन्य processing नहीं करनी चाहिए जो visible Drive document workflow से संबंधित नहीं है।

DynamicMail Google Drive डेटा का उपयोग क्यों करता है

DynamicMail ग्राहक संगठन द्वारा चुने गए Drive document workflows उपलब्ध कराने के लिए Google Drive data का उपयोग करता है। अपेक्षित उद्देश्य हैं:

- अधिकृत users को Drive को document source या destination के रूप में connect करने देना;
- product flow के माध्यम से चुने गए ग्राहक संगठन के business documents को find, list, import, download, export, upload या update करना;
- Drive documents को DynamicMail workflows में extract, classify और route करना;
- अधिकृत ग्राहक संगठन users को connection, file-operation, sync और processing status दिखाना;
- audit records और operational logs रखना जो यह साबित करें कि कौन सा Drive operation अनुरोधित और पूरा किया गया;
- लागू policies और ग्राहक संगठन के agreement द्वारा अनुमत troubleshooting, security, abuse prevention, dispute handling और legal-compliance activities करना।

DynamicMail को Google Drive data बेचना, उसे advertising या retargeting के लिए उपयोग करना, उसे data brokers को transfer करना, surveillance के लिए उपयोग करना, या creditworthiness या lending eligibility निर्धारित करने के लिए उपयोग करना मना है।

Broad scope और narrowest-scope note

<https://www.googleapis.com/auth/drive/scope> broad है क्योंकि यह connected account को उपलब्ध सभी Drive files तक access की अनुमति दे सकता है। DynamicMail इस scope का उपयोग implemented Data Rooms workflow के लिए करता है, जहाँ authorized tenant users selected existing Google Drive folders और files sync करते हैं, Drive content import या download करते हैं, room files को वापस Drive में upload या update करते हैं, और existing Drive files पर user-requested sharing या permission changes लागू करते हैं।

Current workflow के लिए more limited Drive scopes insufficient हैं: `drive.file` केवल DynamicMail द्वारा created या opened files को cover करेगा और selected existing folders या all-files import को cover नहीं करेगा; `drive.readonly` upload, update, sharing या permission changes को cover नहीं करेगा; metadata-only scopes जैसे `drive.metadata.readonly`, `appdata` या `appfolder` tenant document content को download या process नहीं कर सकते और selected existing files को manage नहीं कर सकते। यदि product को Google Picker और केवल app-created या app-opened files के आसपास redesign किया जाता है, तो DynamicMail को उस redesigned workflow की release से पहले scope downscope करना चाहिए।

रिटेंशन

DynamicMail Drive से व्युत्पन्न data केवल visible Drive workflow, ग्राहक संगठन की document retention settings, audit records, security, dispute handling या legal compliance के लिए आवश्यक अवधि तक रखता है। OAuth tokens और Drive operation metadata केवल connected Drive integration को चलाने या required audit records preserve करने के लिए आवश्यक अवधि तक रखे जाते हैं।

Drive file content, cached files, metadata, OCR text, extracted fields और derived document data को तब delete या anonymize कर दिया जाना चाहिए जब वे disclosed purpose के लिए अब आवश्यक न हों, जब तक कि कोई legal, security, audit या customer-retention obligation continuing retention की मांग न करे।

डिलीशन

ग्राहक संगठन का कोई अधिकृत user या administrator Google-derived cached data, imported Drive files, extracted text और derived document records को delete करने का अनुरोध कर सकता है। DynamicMail को ग्राहक संगठन की retention settings और applicable law द्वारा अनुमति मिलने पर requested data delete या anonymize करना चाहिए।

DynamicMail में imported records delete करने से Google Drive में original file आवश्यक रूप से delete नहीं होती। DynamicMail को original Drive files को modify, move, trash या delete केवल तब करना चाहिए जब कोई authorized user visible product workflow के माध्यम से स्पष्ट रूप से वह Drive action अनुरोध करे और वह action ग्राहक संगठन की policy और applicable law द्वारा allowed हो।

रिवोकेशन और डिसकनेक्ट

ग्राहक संगठन DynamicMail में Google Drive को disconnect कर सकता है। disconnect या local consent revocation के बाद, DynamicMail को Google Drive के लिए stored OAuth tokens का उपयोग बंद करना होगा और connected account से additional Drive files को read, write, download, upload, modify या delete करना बंद करना होगा।

Google account owner Google account settings में app authorization भी revoke कर सकता है। यदि Google authorization revoke हो जाता है, तो token refresh या API calls विफल होने पर DynamicMail को Drive API access रोकना होगा, और connection को disconnected या reconnection की आवश्यकता वाले रूप में दिखाया जाना चाहिए।

Local revocation पहले से imported DynamicMail documents को अपने आप नहीं हटाता। उन records को ऊपर दी गई deletion और retention rules के अनुसार संभाला जाता है।

AI, OCR और extraction का उपयोग

DynamicMail Drive file content और metadata पर OCR, parsing, classification, summarization और अन्य AI-assisted processing का उपयोग केवल ग्राहक संगठन के visible Drive document workflow को उपलब्ध कराने या सुधारने के लिए कर सकता है। Drive data और derived data का उपयोग ग्राहक संगठन द्वारा requested feature के बाहर कोई general-purpose machine-learning या AI model बनाने, train करने या improve करने के लिए नहीं किया जाना चाहिए।

AI-assisted results गलत हो सकते हैं। DynamicMail को extracted data को workflow output के रूप में present करना चाहिए जिसे authorized users product flow के अनुसार review, correct, approve, reject या delete कर सकें।

Support और human access

DynamicMail personnel, contractors या subprocessors को specific Drive files, extracted text, file metadata या derived Drive data नहीं पढ़ना चाहिए, जब तक इनमें से कोई condition लागू न हो:

- user ने स्पष्ट रूप से ऐसा support मांगा है जिसके लिए specific data access आवश्यक है;
- security investigation, abuse prevention या incident response के लिए access आवश्यक है;
- law, legal process या ग्राहक संगठन के binding instruction का पालन करने के लिए access आवश्यक है;
- data internal operations के लिए aggregated या anonymized है और किसी specific user की Drive content readable नहीं है।

Support access least-privilege आधारित, जहां practical हो वहां time-limited, और auditability के लिए logged होना चाहिए।

कानूनी समीक्षा स्थिति

स्रोत संदर्भ

- 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>