

Condiții privind accesul la date Google Drive

Aceste condiții explică accesul la date Google Drive pe care DynamicMail îl solicită atunci când un utilizator sau administrator autorizat al tenantului conectează Google Drive pentru fluxurile de lucru cu documente ale tenantului.

Acest text acoperă numai Google Drive. Nu adaugă consultanță juridică specifică unei țări și nu schimbă marcajele aprobate pentru datele de controlor sau pentru revizuirea juridică.

Domeniile de identitate Google Sign-In, precum openid, email și profile, sunt separate de acest consimțământ pentru accesul la date Google Drive. Autentificarea cu Google nu înseamnă acceptarea accesului la Google Drive.

Domeniul de autorizare solicitat

DynamicMail solicită <https://www.googleapis.com/auth/drive> numai atunci când un utilizator sau administrator autorizat al tenantului conectează Google Drive pentru fluxurile de lucru cu documente ale tenantului. Acesta este un domeniu Drive restricționat larg, care poate permite DynamicMail să vizualizeze și să gestioneze toate fișierele din contul Google Drive conectat, inclusiv fișierele deținute de utilizator, fișierele partajate cu utilizatorul, folderele și conținutul unităților partajate disponibil pentru acel cont.

DynamicMail trebuie să folosească domeniul Drive numai pentru fluxurile de lucru Drive cu documente vizibile și comunicate, selectate de tenant. DynamicMail nu trebuie să solicite, să parcurgă, să copieze, să descarce, să modifice, să șteargă sau să proceseze în alt mod date Drive care nu au legătură cu fluxul de lucru Drive vizibil.

Date la care DynamicMail poate avea acces

Atunci când Google Drive este conectat, DynamicMail poate accesa datele Drive necesare pentru a furniza fluxul de lucru selectat de tenant, inclusiv:

- ID-uri de fișiere, nume, tipuri MIME, sume de control, dimensiuni, marcaje temporale, descrieri, etichete, referințe la foldere, foldere părinte și alte metadate ale fișierelor;
- metadate de foldere, metadate ale unităților partajate și rezultate de căutare sau listare necesare pentru localizarea documentelor tenantului;
- conținut de fișiere, previzualizări, miniaturi, exporturi, descărcări, încărcări și conținuturi de fișier generate sau editate;

- metadata de partajare și permisiuni atunci când sunt necesare pentru afișarea sau finalizarea unei operațiuni Drive vizibile asupra unui fișier;
- informații rezumative la nivelul contului Drive necesare pentru confirmarea contului conectat și a stării conexiunii;
- copii stocate sau extrase memorate în cache ale fișierelor Drive importate în DynamicMail;
- date derivate create din fișiere Drive, precum text OCR, câmpuri de document analizate, etichete de clasificare, rezultate de extragere, rezumate, evenimente de audit și înregistrări de documente.

Scopul utilizării

DynamicMail folosește date Google Drive pentru a furniza fluxurile de lucru cu documente Drive selectate de tenant. Scopurile prevăzute sunt:

- permiterea utilizatorilor autorizați să conecteze Drive ca sursă sau destinație pentru documente;
- găsirea, listarea, importarea, descărcarea, exportarea, încărcarea sau actualizarea documentelor comerciale ale tenantului selectate prin fluxul produsului;
- extragerea, clasificarea și direcționarea documentelor Drive în fluxurile de lucru DynamicMail;
- afișarea stării conexiunii, operațiunilor asupra fișierelor, sincronizării și procesării pentru utilizatorii autorizați ai tenantului;
- menținerea înregistrărilor de audit și a jurnalelor operaționale care dovedesc ce operațiune Drive a fost solicitată și finalizată;
- activități de depanare, securitate, prevenire a abuzurilor, gestionare a litigiilor și conformitate juridică permise de politicile aplicabile și de acordul cu tenantul.

DynamicMail nu trebuie să vândă date Google Drive, să le folosească pentru publicitate sau retargeting, să le transfere către brokeri de date, să le folosească pentru supraveghere sau să le folosească pentru determinarea bonității ori a eligibilității pentru creditare.

Notă privind domeniul Drive larg și cel mai restrâns domeniu

Domeniul <https://www.googleapis.com/auth/drive> este larg deoarece poate permite acces la toate fișierele Drive disponibile pentru contul conectat. DynamicMail trebuie să trateze acest domeniu ca provizoriu până când revizuirea de produs și conformitate documentează de ce domeniile Drive mai restrânse nu sunt suficiente pentru fluxul de lucru implementat.

Înainte de utilizarea în producție, DynamicMail trebuie să evalueze domenii Drive mai restrânse, precum `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` sau

drive.appfolder. Dacă un domeniu mai restrâns poate susține funcția vizibilă, domeniul solicitat, înregistrările de consimțământ, configurația OAuth, activul sursă, activul randat și testele trebuie actualizate înainte de lansare.

Păstrare

DynamicMail păstrează datele derivate din Drive numai atât timp cât este necesar pentru fluxul de lucru Drive vizibil, setările de păstrare a documentelor ale tenantului, înregistrările de audit, securitate, gestionarea litigiilor sau conformitate juridică. Tokenurile OAuth și metadatele operațiunilor Drive sunt păstrate numai atât timp cât este necesar pentru operarea integrării Drive conectate sau pentru păstrarea înregistrărilor de audit cerute.

Conținutul fișierelor Drive, fișierele memorate în cache, metadatele, textul OCR, câmpurile extrase și datele de document derivate trebuie șterse sau anonimizate atunci când nu mai sunt necesare pentru scopul comunicat, cu excepția cazului în care o obligație juridică, de securitate, de audit sau de păstrare a tenantului impune păstrarea lor în continuare.

Ștergere

Un utilizator sau administrator autorizat al tenantului poate solicita ștergerea datelor Google memorate în cache, a fișierelor Drive importate, a textului extras și a înregistrărilor de documente derivate. DynamicMail trebuie să șteargă sau să anonimizeze datele solicitate atunci când setările de păstrare ale tenantului și legea aplicabilă permit acest lucru.

Ștergerea înregistrărilor importate în DynamicMail nu șterge neapărat fișierul original din Google Drive. DynamicMail trebuie să modifice, să mute, să trimită în coșul de gunoi sau să șteargă fișiere Drive originale numai atunci când un utilizator autorizat solicită în mod explicit acea acțiune Drive printr-un flux de produs vizibil și acțiunea este permisă de politica tenantului și de legea aplicabilă.

Revocare și deconectare

Tenantul poate deconecta Google Drive în DynamicMail. După deconectare sau revocarea locală a consimțământului, DynamicMail trebuie să înceteze folosirea tokenurilor OAuth stocate pentru Google Drive și trebuie să înceteze citirea, scrierea, descărcarea, încărcarea, modificarea sau ștergerea altor fișiere Drive din contul conectat.

Proprietarul contului Google poate, de asemenea, revoca autorizarea aplicației din setările contului Google. Dacă autorizarea Google este revocată, DynamicMail trebuie să înceteze accesul la API-ul Drive atunci când reîmprospătarea tokenului sau apelurile API eșuează, iar conexiunea trebuie afișată ca deconectată sau ca necesitând reconectare.

Revocarea locală nu elimină automat documentele DynamicMail deja importate. Aceste înregistrări sunt gestionate conform regulilor de ștergere și păstrare de mai sus.

Utilizarea AI, OCR și extragerii

DynamicMail poate folosi OCR, analiză, clasificare, rezumare și alte procese asistate de AI asupra conținutului și metadatelor fișierelor Drive numai pentru a furniza sau îmbunătăți fluxul de lucru vizibil cu documente Drive al tenantului. Datele Drive și datele derivate nu trebuie folosite pentru a crea, antrena sau îmbunătăți un model de învățare automată sau AI cu scop general în afara funcției solicitate de tenant.

Rezultatele asistate de AI pot fi greșite. DynamicMail trebuie să prezinte datele extrase ca rezultat al fluxului de lucru, pe care utilizatorii autorizați îl pot revizui, corecta, aproba, respinge sau șterge conform fluxului produsului.

Acces de suport și acces uman

Personalul DynamicMail, contractorii sau subprocesatorii nu trebuie să citească fișiere Drive specifice, text extras, metadate ale fișierelor sau date Drive derivate, cu excepția cazului în care se aplică una dintre următoarele condiții:

- utilizatorul a solicitat în mod explicit suport care necesită acces la date specifice;
- accesul este necesar pentru o investigație de securitate, prevenirea abuzurilor sau răspuns la incidente;
- accesul este necesar pentru respectarea legii, a unui proces juridic sau a unei instrucțiuni obligatorii a tenantului;
- datele sunt agregate sau anonimizate pentru operațiuni interne și conținutul Drive al unui utilizator specific nu poate fi citit.

Accesul de suport trebuie să urmeze principiul celui mai mic privilegiu, să fie limitat în timp atunci când este practic și să fie înregistrat pentru auditabilitate.

Starea revizuirii juridice

Este material de implementare și localizare, nu consultanță juridică finală și nu consultanță juridică locală. Fără dovezi separate de revizuire, nu trebuie prezentat ca având aprobare Google, aprobare din partea unui consilier juridic extern sau autorizare pentru utilizare în producție cu domeniu restricționat.

Referințe sursă

- 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>