

Gmail tikai lasīšanas datu piekļuves noteikumi

Šajos noteikumos ir paskaidrota Gmail ienākošo dokumentu piekļuve, ko DynamicMail pieprasa, kad pilnvarots klienta organizācijas lietotājs vai administrators pievieno Gmail ienākošo dokumentu apstrādei.

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

Pieprasītais tvērums

DynamicMail pieprasa <https://www.googleapis.com/auth/gmail.readonly> tikai tad, kad pilnvarots klienta organizācijas lietotājs vai administrators pievieno Gmail ienākošo dokumentu saņemšanai. Šis ierobežotais Gmail tvērums ļauj DynamicMail skatīt pievienotā Google konta Gmail ziņojumus un iestatījumus. DynamicMail izmanto šo tvērumu tikai lasīšanas režīmā ienākošajai apstrādei un neizmanto to Gmail ziņojumu sūtīšanai, mainīšanai, dzēšanai, arhivēšanai, marķēšanai ar etiķetēm vai pārvietošanai.

DynamicMail nedrīkst pieprasīt vai apstrādāt Gmail datus, kas nav saistīti ar redzamo ienākošo dokumentu saņemšanas funkciju.

Dati, kuriem DynamicMail var piekļūt

Kad Gmail ienākošais savienojums ir pievienots, DynamicMail var piekļūt Gmail datiem, kas nepieciešami ienākošo biznesa dokumentu atrašanai un apstrādei, tostarp:

- ziņojumu ID, pavedienu ID, vēstures ID, etiķešu atsaucēm un sinhronizācijas kursoriem;
- sūtītājam, saņēmējam, tematam, datumam, galvenēm un citiem ziņojuma metadatiem;
- ziņojuma tekstam un fragmentiem, kas nepieciešami dokumenta konteksta noteikšanai;
- pielikumiem un iegultajiem failiem, kuros var būt rēķini, paziņojumi, vienošanās, kvītis vai citi klienta organizācijas dokumenti;
- Gmail iestatījumiem tikai tiktāl, cik Gmail API tos prasa tikai lasīšanas tvērumam vai konta sinhronizācijas darbībai;
- no Gmail satura izveidotiem atvasinātiem datiem, piemēram, OCR tekstam, parsētiem dokumentu laukiem, klasifikācijas etiķetēm, izgūšanas rezultātiem, kopsavilkumiem, audita notikumiem un dokumentu ierakstiem.

Izmantošanas nolūks

DynamicMail izmanto Gmail tikai lasīšanas datus, lai nodrošinātu Gmail ienākošo dokumentu avotu, ko izvēlējusies klienta organizācija. Paredzētie nolūki ir:

- noteikt ienākošos ziņojumus, kuros var būt klienta organizācijas biznesa dokumenti;
- importēt pielikumus vai ziņojuma saturu, ko klienta organizācija izvēlas apstrādāt;
- izgūt, klasificēt un novirzīt dokumentus DynamicMail darbplūsmās;
- saskaņot sinhronizācijas stāvokli, lai viens un tas pats ziņojums netiktu importēts atkārtoti;
- rādīt savienojuma, sinhronizācijas un apstrādes statusu pilnvarotiem klienta organizācijas lietotājiem;
- veikt problēmu novēršanas, drošības, audita un tiesiskās atbilstības darbības, ko atļauj piemērojamās politikas un klienta organizācijas līgums.

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

Glabāšana

DynamicMail glabā no Gmail iegūtos datus tikai tik ilgi, cik tas nepieciešams redzamajai ienākošo dokumentu funkcijai, klienta organizācijas dokumentu glabāšanas iestatījumiem, audita ierakstiem, drošībai, strīdu izskatīšanai vai tiesiskajai atbilstībai. OAuth piekļuves marķieri un sinhronizācijas metadati tiek glabāti tikai tik ilgi, cik tie nepieciešami pievienotā Gmail ienākošā avota darbībai vai nepieciešamo audita ierakstu saglabāšanai.

Neapstrādāts Gmail ziņojumu saturs, pielikumi 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 pielikumus, 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 e-pasta ziņojumu vai pielikumu no Gmail, jo Gmail tikai lasīšanas tvērums nepiešķir DynamicMail tiesības mainīt vai dzēst Gmail ziņojumus.

Atsaukšana un atvienošana

Klienta organizācija var atvienot Gmail ienākošo savienojumu DynamicMail sistēmā. Pēc atvienošanas vai vietējās piekrišanas atsaukšanas DynamicMail vairs nedrīkst izmantot saglabātos OAuth piekļuves marķierus Gmail ienākošajam avotam un vairs nedrīkst lasīt papildu Gmail ziņojumus no pievienotā konta.

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

Vietējā atsaukšana 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 Gmail izcelsmes ziņojumu saturam un pielikumiem tikai tādēļ, lai nodrošinātu vai uzlabotu klienta organizācijai redzamo ienākošo dokumentu darbplūsmu. Gmail 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, darbuzņēmēji vai apakšapstrādātāji nedrīkst lasīt konkrētus Gmail ziņojumus, pielikumus, izgūto tekstu vai atvasinātos Gmail 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 Gmail 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>
- Gmail API scopes: <https://developers.google.com/workspace/gmail/api/auth/scopes>
- Google restricted-scope verification guidance:
<https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification>