

Warunki dostępu do danych Gmail tylko do odczytu

Te warunki wyjaśniają dostęp do Gmaila, o który prosi DynamicMail, gdy upoważniony użytkownik lub administrator tenanta podłącza przyjmowanie dokumentów z Gmaila.

Zakresy tożsamości Google Sign-In, takie jak `openid`, `email` i `profile`, są oddzielne od tej zgody na dostęp do danych Gmaila. Zalogowanie się przez Google nie oznacza akceptacji dostępu do przyjmowania dokumentów z Gmaila.

Żądany zakres

DynamicMail prosi o `https://www.googleapis.com/auth/gmail.readonly` tylko wtedy, gdy upoważniony użytkownik lub administrator tenanta podłącza przyjmowanie dokumentów z Gmaila. Ten ograniczony zakres Gmaila pozwala DynamicMail wyświetlać wiadomości i ustawienia połączonego konta Gmail.

DynamicMail używa tego zakresu do przetwarzania tylko do odczytu. DynamicMail nie używa go do wysyłania, modyfikowania, usuwania, archiwizowania, oznaczania etykietami ani przenoszenia wiadomości Gmail.

DynamicMail nie powinien żądać ani przetwarzać danych Gmaila, które nie są związane z widoczną funkcją przyjmowania dokumentów z Gmaila.

Dane, do których DynamicMail może mieć dostęp

Gdy przyjmowanie dokumentów z Gmaila jest podłączone, DynamicMail może mieć dostęp do danych Gmaila potrzebnych do wyszukiwania i przetwarzania przychodzących dokumentów biznesowych, w tym do:

- identyfikatorów wiadomości, identyfikatorów wątków, identyfikatorów historii, odwołań do etykiet i kursorów synchronizacji;
- nadawcy, odbiorcy, tematu, daty, nagłówek i innych metadanych wiadomości;
- treści wiadomości i fragmentów potrzebnych do rozpoznania kontekstu dokumentu;
- załączników i plików osadzonych, które mogą zawierać faktury, powiadomienia, umowy, potwierdzenia lub inne dokumenty tenanta;
- ustawień Gmaila tylko wtedy, gdy Gmail API wymaga ich dla zakresu tylko do odczytu lub dla działania synchronizacji konta;
- danych pochodnych utworzonych z treści Gmaila, takich jak tekst OCR, sparsowane pola dokumentów, etykiety klasyfikacji, wyniki ekstrakcji, podsumowania, zdarzenia audytowe i rekordy dokumentów.

Cel użycia

DynamicMail używa danych Gmaila tylko do odczytu, aby udostępnić źródło przyjmowania z Gmaila wybrane przez tenanta. Zamierzone cele obejmują:

- wykrywanie przychodzących wiadomości, które mogą zawierać dokumenty biznesowe tenanta;
- importowanie załączników lub treści wiadomości, które tenant wybiera do przetwarzania;
- wyodrębnianie, klasyfikowanie i kierowanie dokumentów do przepływów pracy DynamicMail;
- uzgadnianie stanu synchronizacji, aby ta sama wiadomość nie była importowana wielokrotnie;
- pokazywanie upoważnionym użytkownikom tenanta stanu połączenia, synchronizacji i przetwarzania;
- rozwiązywanie problemów oraz działania związane z bezpieczeństwem, audytem i zgodnością prawną dozwolone przez obowiązujące zasady i umowę z tenantem.

DynamicMail nie może sprzedawać danych Gmaila, używać ich do reklam lub retargetingu, przekazywać ich brokerom danych, używać ich do nadzoru ani używać ich do ustalania zdolności kredytowej lub kwalifikowalności do pożyczki.

Przechowywanie

DynamicMail przechowuje dane pochodzące z Gmaila tylko tak długo, jak jest to potrzebne dla widocznej funkcji przyjmowania dokumentów, ustawień przechowywania dokumentów tenanta, zapisów audytowych, bezpieczeństwa, obsługi sporów lub zgodności prawnej. Tokeny OAuth i metadane synchronizacji są przechowywane tylko tak długo, jak są potrzebne do działania podłączonego źródła przyjmowania z Gmaila lub do zachowania wymaganych zapisów audytowych.

Surowa treść wiadomości Gmail, załączniki i pochodne dane dokumentów powinny zostać usunięte lub zanonimizowane, gdy nie są już potrzebne do ujawnionego celu, chyba że obowiązek prawny, bezpieczeństwa, audytu lub przechowywania określony przez tenanta wymaga dalszego przechowywania.

Usuwanie

Upoważniony użytkownik lub administrator tenanta może zażądać usunięcia buforowanych danych pochodzących z Google, zaimportowanych załączników, wyodrębnionego tekstu i pochodnych rekordów dokumentów. DynamicMail powinien usunąć lub zanonimizować żądane dane, gdy pozwalają na to ustawienia przechowywania tenanta i obowiązujące prawo.

Usunięcie zaimportowanych rekordów DynamicMail nie musi usuwać oryginalnej wiadomości e-mail ani załącznika z Gmaila, ponieważ zakres Gmail tylko do odczytu nie daje DynamicMail uprawnienia do modyfikowania ani usuwania wiadomości Gmail.

Cofnięcie zgody i odłączenie

Tenant może odłączyć przyjmowanie dokumentów z Gmaila w DynamicMail. Po odłączeniu lub lokalnym cofnięciu zgody DynamicMail musi przestać używać przechowywanych tokenów OAuth dla przyjmowania z Gmaila i musi przestać czytać dodatkowe wiadomości Gmail z połączonego konta.

Właściciel konta Google może także cofnąć autoryzację aplikacji w ustawieniach konta Google. Jeśli autoryzacja Google zostanie cofnięta, DynamicMail musi zatrzymać dostęp do Gmail API, gdy odświeżenie tokenu lub wywołania API się nie powiedą, a połączenie powinno być pokazane jako odłączone lub wymagające ponownego połączenia.

Lokalne cofnięcie zgody nie usuwa automatycznie już zaimportowanych dokumentów DynamicMail. Te rekordy są obsługiwane zgodnie z powyższymi zasadami usuwania i przechowywania.

AI, OCR i ekstrakcja

DynamicMail może używać OCR, parsowania, klasyfikacji, podsumowywania i innego przetwarzania wspomaganego przez AI na treści wiadomości i załącznikach pochodzących z Gmaila tylko w celu udostępnienia lub ulepszenia widocznego przepływu pracy przyjmowania dokumentów dla tenanta. Dane Gmaila i dane pochodne nie mogą być używane do tworzenia, trenowania ani ulepszania ogólnego modelu uczenia maszynowego lub AI poza funkcją zamówioną przez tenanta.

Wyniki wspomagane przez AI mogą być błędne. DynamicMail powinien prezentować wyodrębnione dane jako wynik przepływu pracy, który upoważnieni użytkownicy mogą sprawdzać, poprawiać, zatwierdzać, odrzucać lub usuwać zgodnie z przepływem produktu.

Wsparcie i dostęp człowieka

Personel, wykonawcy lub podprocesorzy DynamicMail nie powinni czytać konkretnych wiadomości Gmail, załączników, wyodrębnionego tekstu ani pochodnych danych Gmaila, chyba że zachodzi jeden z poniższych warunków:

- użytkownik wyraźnie poprosił o wsparcie wymagające dostępu do konkretnych danych;
- dostęp jest niezbędny do dochodzenia bezpieczeństwa, zapobiegania nadużyciom lub reagowania na incydent;
- dostęp jest niezbędny do przestrzegania prawa, procesu prawnego lub wiążącej instrukcji tenanta;

- dane są zagregowane lub zanonimizowane na potrzeby wewnętrznych operacji, a treść Gmaila konkretnego użytkownika nie jest możliwa do odczytania.

Dostęp wsparcia powinien być oparty na zasadzie najmniejszych uprawnień, w praktycznym zakresie ograniczony czasowo i rejestrowany na potrzeby audytu.

Jest to lokalizowany materiał wdrożeniowy i przeglądowy, a nie ostateczna porada prawna ani lokalna porada prawna. Bez osobnego dowodu oceny nie wolno przedstawiać go jako mającego poparcie Google, akceptację zewnętrznego doradcy prawnego lub produkcyjne dopuszczenie restricted-scope.

Referencje

- 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>